Uses of AI in migration and border control:
A fundamental rights approach to the Artificial Intelligence Act

Artificial Intelligence (AI) systems are increasingly developed and deployed for purposes related to migration, asylum and border control.[1] However, the use of AI in such contexts leads to severe intrusions on fundamental rights and broader societal concerns as to the testing and use of invasive systems on marginalised people, such as migrants and people on the move.[2]

Amendment summary:

This document outlines the following amendments to the European Commission's proposed Artificial Intelligence Act (AIA), to ensure fundamental rights protection for people subjected to AI systems in the migration control context:

1. Include a recital upholding international obligations in the field of migration and international protection;
2. AI-based individual risk assessment and profiling systems:
   A. Prohibit the use of AI-based individual risk assessment and profiling systems in a migration context;
   B. Ensure other AI-based risk assessments are classified as 'high-risk' in Annex III;
3. Prohibit AI Polygraphs and similar tools in migration management;
4. Predictive analytic systems:
   A. Include as 'high-risk' Annex III predictive analytic systems in migration, asylum and border control management;
   B. Prohibit predictive analytics for the purpose of interdicting, curtailing and preventing migration;
5. Biometrics in the migration context:
   A. Include as 'high-risk' Annex III Biometric Identification systems in migration, asylum and border control management;
   B. Prohibit Remote Biometric Identification in publicly accessible spaces;
   C. Prohibit Remote Biometric Categorisation in publicly accessible spaces, and any discriminatory Biometric Categorisation;
6. Include as 'high-risk' in Annex III AI systems used for monitoring and surveillance in border control;
7. Ensure AI for the assessment of evidence is 'high-risk' and is included in Annex III;

---

[1] Petra Molnar and Lex Gill, "Bots at the Gate: A Human Rights Analysisof Automated Decision-Making in Canada's Immigration and Refugee System," (University of Toronto International Human Rights Program and the Citizen Lab, Munk School of Global Affairs, 2018) https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-AutomatedSystems-Report-Web-V2.pdf; Vavoula, N. (2021). Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism, European Journal of Migration and Law, 23(4), 457-484. doi: https://doi.org/10.1163/15718166-12340114

[2] UN Special Rapporteur on Contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Report to the 75th session of the UN General Assembly. November 2020 https://undocs.org/A/75/590

This paper was drafted by Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch. It is supported by the European Centre for non-profit Law (ECNL), European Disability Forum (EDF), Privacy International. It follows the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.

8. Amend Article 83 to ensure AI as part of large-scale EU IT databases are within the scope of the AIA.

1. Recital: Upholding international obligations in the field of migration and international protection

The use of AI in the context of migration raises a broad range of structural and fundamental rights considerations. It is crucial that uses of AI in migration control in no way enable a contravention of international obligations, in particular relating to the international law principle of non-refoulement and other foundational principles of international refugee and human rights law.

2. AI-based individual risk assessments

(2.A) Prohibit in Article 5 the use of AI-based individual risk assessment and profiling systems in a migration context

Use cases: AI- based individual risk assessment

- The **'visa streaming' algorithm** was used by the UK Home Office to filter visa applications. In 2020, following a legal challenge, the algorithm was suspended as it "entrenched racism and bias into the visa system", according to the UK Home Office itself.

- The **ETIAS Regulation** enables profiling to categorise travellers into pre-defined risk profiles related to purported migration, security or public health risks. This profiling takes place with a number of factors, including historical data on rates of over-staying or refusal and information provided by Member States as to security risks.
  See Niovi Vavoula, 'The Commission Package for ETIAS Consequential Amendments – Substitute Impact Assessment' (2020) 20–30.

AI-based risk assessment and profiling systems are used to assess individuals for risks to public security, irregular migration, public health, and also to predict people's behaviour. In the context of migration and border checks, these AI systems are then used to assess travellers on the basis of pre-defined risk categories, filtering legitimate from illegitimate travellers, with the ultimate goal of preventing the latter from entering or residing on EU territory. Risk-assessments are also used in automated surveillance systems in refugee camps and in border contexts.[3]

Violations of rights to non-discrimination and equality

[3] See sections 4 and 6.

This paper was drafted by Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch. It is supported by the European Centre for non-profit Law (ECNL), European Disability Forum (EDF), Privacy International. It follows the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.

AI-based individual risk assessment systems assess and profile people based on predetermined risk indicators embedded in screening rules, parameters which are often opaque and not made public. The use of automated risk assessment and profiling systems during migration procedures is a dangerous practice that poses a serious threat to the right to non-discrimination, both directly and indirectly.

Such systems by nature violate the right to non-discrimination in the migration context insofar as they codify assumptions about the link between personal data and characteristics with particular risks. People are not judged on individual behaviour or on factors within their control, but rather by pre-determined characteristics, such as nationality.[4] This is the very essence of what non-discrimination law seeks to prevent and prohibit. These forms of discrimination are prohibited in the EU Charter of Fundamental Rights and Freedoms, international racial discrimination law, and under international human rights law.[5]

Even if the automated analysis is conducted on non-sensitive data only, sensitive data can be inferred by proxy, creating a demonstrable risk of **indirect discrimination.** For example, geographic location may reveal a person's probable ethnicity, and nationality could be a proxy for race or religion, protected characteristics under EU law. Furthermore, processing based on education levels (as in ETIAS) and job groups open up the potential for unlawful discriminatory profiling. As such, outcomes may resemble that of using risk indicators directly based on sensitive data, which is prohibited. As highlighted by the UN Special rapporteur on Racism, AI-based risk assessment and profiling in the migration context are likely to have indirect discriminatory effect on a group of people that share the same protected characteristics.[6] The European Court of Justice[7] also highlighted to the discrimination risks in the context of automated decision-making.

<u>Violations of the right to privacy, data protection and procedural rights</u>

The application of algorithmic profiling also infringes a number of subsequent fundamental rights, such as the right to private and family life, the right to personal data protection, the right to a fair trial and the presumption of innocence, as well as the right to an effective remedy. The use of such risk assessments is inherently opaque in the migration context, and will be almost impossible to challenge considering the imbalances of power in which they are deployed. Individuals affected have no mechanism to access the parameters on which these risk assessments are based, or to challenge them for discriminatory or incorrect outcomes, which could amount to a number of consequential, irrevocable, life altering and harmful decisions, including detention and deportation.

---

4 Niovi Vavolua "Immigration and Privacy in the Law of the European Union – The Case of Information Systems (forthcoming 2022)

5 UN Convention for the elimination of all forms of racial discrimination, ; EU Charter of fundamental rights, Article 21; UN Convention on the Rights of Persons with Disabilities, Article 5.; UN Convention Relating to the Status of Refugees (Refugee Convention); Protocol Relating to the Status of Refugees; International Covenant on Civil and Political Rights Article 9; Universal Declaration of Human Rights Article 3; Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; Convention on the Rights of Persons with Disabilities Article 14; Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW); Convention on the Rights of the Child; International Convention on the Elimination of All Forms of Racial Discrimination

6 Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (2020) *Racial and xenophobic discrimination, emerging digital technologies, and border and immigration enforcement*, (A/HRC/44/57).

7 Opinion 1/15 (EU:C:2017:592); *La Quadrature du Net and Others v Premier Ministre and Others, (*C-520/18).

This paper was drafted by Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch. It is supported by the European Centre for non-profit Law (ECNL), European Disability Forum (EDF), Privacy International. It follows the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.

In many cases these systems violate the essence of a number of data protection principles, including the need for informed consent[8] for the processing of personal data, and the principle of purpose limitation. On the question of consent, data taken in the migration context is more accurately 'extracted' from people on the move, who often have no choice but to submit to the process. In this context, the data subject can never effectively freely give specific and informed consent to the data processing for particular purposes, because those purposes are constantly changing in a way that cannot be foreseen by individual subjects.[9] On the issue of purpose limitation, the governance of migration databases, at EU and national level, is constantly in flux, with the political system constantly shifting the purposes for which these systems exist and collect data. This state of constant change of purposes prevents individuals subject to them having a clear understanding of the purpose for which the data is used.

Due to the opacity of decision-making and extreme power imbalance in the migration context, no safeguards can mitigate these violations of rights to non-discrimination, privacy, data protection and procedural rights. Transparency and data quality provisions cannot address the inherent harms these systems pose for people on the move.

For these reasons, risk profiling in the context of migration should be added to the list of prohibited practices in Article 5.

(2.B) Ensure other AI-based risk assessments are classified as 'high-risk'

Furthermore, AI systems to assess different types of risk relating to the migration context may be developed and deployed in the future. Regardless of the type of risk being assessed, the fundamental rights of people on the move are seriously impacted insofar as the assessment affects their outcomes and treatment in the migration process.

A particular concern is that AI-based risk assessments significantly alter, based on discriminatory assumptions, the fundamental principle that migration and asylum procedures must be based on objective evidence and tailored to the needs of the individual. Such assessments are highly complex and contextual, and in some cases must be completed through individual needs assessments to provide scope for the identification of vulnerabilities, requiring significant resources and multidisciplinary teams. If AI systems are developed and deployed to assist these purposes, they must be subject to the requirements on AI systems within the AI Act.

In addition, the use of AI systems to conduct individual risk assessments and profiling is likely to undermine Article 5(1)(d) of the GDPR with respect to the quality of personal data. Poor or inaccurate data quality is a

---

8 As defined in the GDPR, Recital 32 consent is defined as a clear affirmative act establishing a "freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her".

9 For example, the EURODAC system is currently shifting from a database with the purpose of determining where claims of international protection should be made to a database for law enforcement access. See EDRi (2021). Intensified surveillance at EU borders: EURODAC reform needs a radical policy shift: https://edri.org/our-work/intensified-surveillance-at-eu-borders-eurodac-reform-needs-a-radical-policy-shift/

particular issue of concern in relation to the data available in EU migration databases. Rather than improving data quality by proposing more data collection, thus undermining principles of consent and purpose limitation, these systems should be accepted as posing an unacceptable risk to fundamental rights.[10]

3. AI polygraphs and emotion recognition in the migration context

AI polygraphs (i.e. 'lie detectors') and 'emotion recognition' technologies are a type of system claiming to infer someone's emotional state, or intention or the state of mind (such as 'deception', 'trustworthiness' or 'truthfulness') of natural persons on the basis of their biometric data, or other data relating to their physical, physiological or behavioural characteristics. Such systems have been used to purportedly detect people's intentions and emotions throughout the migration process, mainly to assess the credibility of their statement.

Use Cases: AI polygraphs

- **iBorderCtrl project:** This systems aims at enabling faster and more thorough border control for third country nationals crossing the land borders of EU Member States. It includes the deployment of the **Automatic Deception Detection System** (ADDS) which performs, controls and assesses the pre-registration interview by sequencing a series of questions posed to travellers by an Avatar. The ADDS quantifies the probability of deceit by analysing interviewees' non-verbal micro-gestures and verbal communication.

- **Automated Virtual Agent for Truth Assessments in Real-Time** (**AVATAR**): It is a system designed to automate screening, interviewing and credibility assessment of persons crossing international borders. The system was developed by the BORDERS research center of the University of Arizona, with the support of FRONTEX and the US Department of Homeland Security. During the automated screening and interviews, the AVATAR lie-detector system measures changes in eye movements, pupil dilation and voice quality in order to identify potential risk individuals. According to Frontex itself, '[...] the performance of AVATAR and other similar systems becomes dubious due to the risk of algorithmic biases'.

  Frontex letter: CBD/RIU/DRVO/11337/2019, in response to parliamentary question E-002653/2019 by MEP Özlem Demirel (GUE/NGL) Frontex, "Artificial Intelligence - based capabilities for European Border and Coast Guard" (2021), 100

AI polygraphs in the migration context represent an unacceptable risk on several levels.[11]

[10] EU Fundamental Rights Agency (FRA) 'Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security' (2017) 30; FRA, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights' (2018) 81–94.

[11] Niovi Vavoula, 'Unpacking the EU proposal for an AI Act: implications for AI systems used in the context of migration, asylum and border control management', Turkish Policy Quarterly (4 March 2022), http://turkishpolicy.com/article/1100/unpacking-the-eu-proposal-for-an-ai-act-implications-for-ai-systems-used-in-the-context-of-migration-asylum-and-border-control-management

Firstly, they have the potential to infringe the right to non discrimination, as they claim to infer a person's behaviour based on problematic assumptions about human behavior, which are grounded in Western notions of truthfulness and deception.[12] Because of the intrinsic bias of these technologies, there is a great risk that such systems will misinterpret cultural signifiers that do not match those that they were trained on.[13] These assumptions exacerbate existing, problematic conceptions of credibility in the migration context, in which a wider context of disbelief and racialised suspicion has been cultivated against people on the move, as a strategy to prevent or combat 'irregular' migration. Moreover, it has been shown that facial recognition technology, which is often used in emotion recognition systems, tends to perform worse on people with darker skin tones, on women, and most significantly on racialised women.[14]

Secondly, the scientific foundations of emotion recognition systems have been called into question, such that there are serious doubts about whether current systems, and even future systems, can actually do what they claim.[15] Criticisms have long been leveled against 'traditional' polygraphs, and the evidence for their effectiveness is far from convincing. Automating already dubious approaches to detecting deception using machine learning or other AI techniques will not alleviate, and likely worsen, their potential to cause harm.[16]

Thirdly, AI polygraphs represent a highly invasive form of surveillance that hampers a wide range of fundamental rights.[17] The use of these systems represent a gross violation in the context of migration procedures risks undermining several human rights, such as the right to privacy, freedom of thought,[18] the right to asylum, a fair trial, as well as the right to an effective remedy and other procedural rights such as the presumption of innocence and the right to a fair and impartial decision-maker. In the context of migration decision-making, AI polygraphs risk unduly affecting the procedure, as their results are used by the responsible authority to influence the decision-making process, consequently impeding the full exercise of the rights of the concerned person.

(3) Prohibit AI Polygraphs and similar tools in migration management

---

12 Krys, K., Melanie Vauclair, C., Capaldi, C.A. et al. Be Careful Where You Smile: Culture Shapes Judgments of Intelligence and Honesty of Smiling Individuals. J Nonverbal Behav 40, 101–116 (2016). https://doi.org/10.1007/s10919-015-0226-4

13 Raji, Deborah 'How our data encodes systematic racism', MIT Technology Review, 10 December 2020, https://www.technologyreview.com/2020/12/10/1013617/racism-data-science-artificial-intelligence-ai-opinion/

14 Lauren Rhue, 'Emotion-reading tech fails the racial bias test', The Conversation, 3 January 2019, https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404

15 Barrett et al., 2019, Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, https://doi.org/10.1177/1529100619832930 https://journals.sagepub.com/stoken/default+domain/10.1177%2F1529100619832930-FREE/pdf

16 Courtney Hinkle, 'The Modern Lie Detector: AI-Powered Affect Screening and the Employee Polygraph Protection Act (EPPA)', THE GEORGETOWN LAW JOURNAL [Vol. 109:1201] https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2021/06/Hinkle-The_Modern_Law_Detector.pdf

17 Article 19, Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights (November 2020)

18 Susie Alegre, Regulating around freedom in the "forum internum," ERA Forum (2021), Vol. 21: 591-604, DOI: https://doi.org/10.1007/s12027-020-00633-7)

This paper was drafted by Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch. It is supported by the European Centre for non-profit Law (ECNL), European Disability Forum (EDF), Privacy International. It follows the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.

Due to the gravity of the risks posed by AI polygraphs in the migration context, such systems should be prohibited in the Regulation and added to the list of prohibited practices in Article 5.

For a comprehensive position on emotion recognition systems, see the civil society issue paper 'Prohibit emotion recognition in the Artificial Intelligence Act'.

4. Predictive analytic AI systems in migration, asylum and border control management

There is an increase in the development and use of AI-based predictive analytic systems for the purpose of monitoring, forecasting and anticipating migratory or population movements. Such systems utilise data on historical trends and information to make predictions about future migration situations or events.

Predictive analytic systems may deploy a range of methods, including data mining, predictive modelling and machine learning, and process different forms of data including biometric information, social media data, and data in relation to past events and trends.

Use cases: Predictive analytic AI systems in migration, asylum and border control management

- **European Asylum Support Office (EASO) forecasting and early warning tool:** As outlined in a feasibility study, EASO (now European Agency for Asylum (EUAA) outlined work exploring the development of a forecasting and early warning tool based on AI technology, specifically to be used to forecast irregular migration. The tool would purportedly use machine learning to predict pressures on the asylum administrations of member states of the EU. Input and training data to the system would be historical data on past migration trends, social media monitoring data, data on pressures at EU external borders and data on the outcomes of asylum claims.
  European Commission (2020) Feasibility study on a forecasting and early warning tool for migration based on Artificial Intelligence technology; Carammia, Iacus and Wilkin (2022) 'Forecasting asylum-related migration flows with machine learning and data at scale' 12:1457 Nature, https://doi.org/10.1038/s41598-022-05241-8.

- **Centaur**: The Greek Ministry of Migration and Asylum implemented a partly-automated surveillance system, "Centaur" at refugee camps on Lesbos, Chios, Samos, Leros, and Kos. The Centaur system uses a range of surveillance infrastructure, including cameras and motion sensors, and in the future thermal cameras and drones. With the data gathered, Centaur uses an algorithm to predict and flag "threats" (such as the potential presence of weapons, unauthorised visits or behaviour). The results of this assessment trigger various reactions in the central processing centre in Athens based on the purported risk posed.
  Given the fundamental rights concerns, the Greek DPA recently launched an investigation into the deployment of the the Centaur system by the Ministry of the Interior.
  World News, "EU tests digital barriers at migration flashpoint along Greece-Turkey border", Jersey Evening Post, (03 June 2021), online: <jerseyeveningpost.com/news/world-news/2021/06/03/eu-tests-digital-barriers-at-migration-flashpoint-along-greece-turkey-border/>
  Homo Digitalis, "A major success for civil society in Greece: The Hellenic DPA launches an investigation into the Ministry of Immigration and Asylum re the YPERION and KENTAYROS IT systems" (9 March 2022),

---

This paper was drafted by Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch. It is supported by the European Centre for non-profit Law (ECNL), European Disability Forum (EDF), Privacy International. It follows the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.

online: <https://www.homodigitalis.gr/en/posts/11024>

- **Frontex risk analysis:** As described by the European Parliament Research Service, Frontex published a tender for a social media analysis service concerning irregular migration trends and forecasts to support the **planning and evaluation of joint operations.** In a research report released in 2020, Frontex outlines a number of potential use cases for påredictive analytics. The 2021 Commission implementing regulation on the situational pictures of EUROSUR108 provides that Member States and Frontex 'should develop technical interfaces to foster machine to machine interconnections and use decision support tools to assist EUROSUR operators in their tasks'.
  European Parliament Research Service (2021) Artificial Intelligence at EU borders: Overview of applications and key issues:
  https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf
  Frontex 'Artificial Intelligence Based Capabilities for the European Border and Coast Guard':
  https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf

(4.A) Include in Annex III predictive analytic systems in migration, asylum and border control management

Such systems may have vast consequences for fundamental rights and access to international protection procedures, affecting potentially how resources are assessed and allocated in the migration control and international protection contexts. Incorrect assessments about migration trends, reception needs and other relevant concerns, will have significant consequences for the preparedness of Member States, but also for the likelihood that individuals can access international protection, reception needs and numerous other fundamental rights in the context of migration.

In some cases, predictive systems also involve the use of personal data. In these cases, such systems present a challenge to the principle of purpose limitation, consent of the data-subject, data minimization and disproportionate data processing. As outlined by the European Data Protection Supervisor with respect to EASO's tool:

'The processing of personal data from social media - including special categories of personal data, personal data of individuals pertaining to vulnerable groups and personal data potentially related to criminal charges - creates risks to the fundamental rights and freedoms of individuals, including the rights to data protection and privacy, but transcending beyond them and potentially as far as to the right of asylum.'

The EDPS further outlined that migrants and asylum seekers are a vulnerable population and that *'EASO's monitoring activities subject them to enhanced surveillance due to the mere fact that they are or might become migrants or asylum seekers'*, presenting a severe risk of undermining the right to non-discrimination.

Most significantly, predictive analytic systems may have concrete repercussions on fundamental rights insofar as such systems contribute to a wider framework of surveillance of the border and people on the move.

For these reasons, **AI based predictive analytic systems must be included as 'high-risk' and be subjected to the safeguards provided by the AIA.** Their use can present a risk of impacting the fundamental rights to life,

liberty, and security of the person, in addition to non-discrimination, privacy, data protection and the right to asylum. It is vital that such systems are subject to the series of safeguards contained in the AIA, in particular to offer additional oversight and transparency as to the functioning of these systems.

(4.B) Prohibit predictive analytic systems in migration, asylum and border control management for the purpose of interdicting, curtailing and preventing migration

Additional fundamental rights issues arise with respect to the context of use. In many cases, predictive systems will be used in combination with broader surveillance infrastructure. Service providers and human rights defenders supporting people on the move have highlighted the severe dangers posed when technologies are deployed in the practice of pushbacks.[19]

When used with the aim of combating 'irregular migration' such systems threaten the fundamental right to asylum and contravene the international law principle of *non-refoulement*. This customary international law principle guarantees the right to seek asylum and that no person should risk being returned to a country where they would face torture, cruel, inhuman or degrading treatment or punishment and other irreparable harm.[20] Predictive analytic systems may generate assumptions that particular groups of persons are deemed to present a risk of 'irregular migration' and may encourage or facilitate preventative or other responses geared toward interdiction or otherwise halting movement.

As such, deployments of predictive analytic systems for certain purposes amount to an unacceptable risk to fundamental rights and therefore must be prohibited insofar as such systems are used to interdict, curtail or prevent movement. When used for this purpose, such systems by definition undermine the right to seek asylum, the principle of *non-refoulement*, the right to life, integrity, the prohibition of torture and inhuman or degrading treatment or punishment and the right to equal treatment and non-discrimination, insofar as aggregate assessments are used to make highly consequential decisions for individual treatment and access to rights in the course of the migration process. With these examples in mind, include the following in Article 5 prohibited AI practices.

5. Biometrics in the migration context

In the migration context, there are different ways in which AI systems can process data relating to physical, physiological or behavioural characteristics of natural persons, including biometric data.

Given the sensitivity of biometric data, it is vital that the AI Act supports and builds upon the rights-based frameworks of the GDPR and LED to make sure that data about people's faces and bodies cannot be used

---

19 See Border Violence Monitoring Network: submission to the Special Rapporteur on Racism: 'The role of technology in illegal push backs from Croatia to Bosnia-Herzegovina and Serbia': https://www.borderviolence.eu/ohchr-submission-the-role-of-technology-in-illegal-push-backs-from-croatia-to-bosnia-herzegovina-and-serbia/ ; See also Statewatch: https://www.statewatch.org/news/2022/march/pushbacks-in-greece-commission-calls-for-investigations-and-more-border-surveillance/

20 Article 33 Convention and Protocol Relating to the Status of Refugees (1951)

against them, and that stronger safeguards are put in place for their use, in order to address the limitations of the risk-based framework of the AI Act.[21]

(5.A) Include as 'high-risk' in Annex III biometric Identification in migration, asylum and border control management

In the migration context, AI tools are widely used to perform identity checks, both at and within EU borders. The increased use of identity checks is a recurring feature in EU migration policy, in particular as part of a broader strategy to combat identity fraud and to increase the number of deportations.[22] These systems include mobile biometric identification devices that make it possible to scan fingerprints or faces in the streets and automatically compare the biometric data against a database or a watchlist. However, the use of biometric identification systems poses great risks to the fundamental right non-discrimination and it can infringe the principle of proportionality. That racial profiling techniques are a systematic practice across EU law enforcement and migration control authorities is well-documented,[23] and several stakeholders, including the Council of Europe[24] and the Fundamental Rights Agency (FRA)[25], have repeatedly called for the introduction of effective safeguards to end police discriminatory practices. The introduction of biometric identification systems has the worrying potential of further exacerbating discriminatory practices.[26] Further, within the EU Justice and Home Affairs (JHA) objective to increase the number of deportations, biometric

---

21 See separate paper, entitled: Strictly regulate high-risk uses of biometrics in AI systems, drafted by by European Digital Rights (EDRi), Access Now, ARTICLE19, Bits of Freedom, the Chaos Computer Club (CCC), Digitale Gesellschaft CH and the IT-Political Ass Association of Denmark (IT-Pol). Association of Denmark (IT-Pol).

22 Council of the EU, 'Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area: - State of play of its implementation', 8 November 2016, https://www.statewatch. org/media/documents/news/2016/dec/eu-council-info-exhang-interop-sop-13554- REV-1-16.pdf

23 Fundamental Rights Agency, 'Being Black in the EU', 2018, p.30, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-being-black-in-the-eu_en.pdf; Equinox Initiative for Racial Justice, 'Who protects us from the Police? Structural Racism in Law Enforcement in the European Union', Equinox Initiative for Racial Justice, June 2021, https://www.equinox-eu.com/wp-content/uploads/2021/10/Equinox-Who-Protects-Us-from-the-Police.pdf; 'Identificaciones basadas en perfil étnico en Granada', APDHA/Instituto de la paz y los conflictos, 2016, https://www.pareudepararme.org/uploads/2016_Granada_APDHA_identificaciones-etnicas.pdf; 'Statement to the media by the United Nations Working Group of Experts on People of African Descent, on the conclusion of its official visit to Spain, 19-26 February 2018', 26 February 2018, https://www.ohchr.org/en/press-releases/2017/02/committee-elimination-discrimination-against-women-discusses-situation-women?LangID=E&NewsID=21171

24 Council of Europe, Committee on Equality and non-Discrimination. 'Ethnic profiling in Europe: a matter of great concern', 14 December 2020,

25 FRA, 'Second European Union Minorities and Discrimination Survey. Main results', 2017, https://fra.europa.eu/sites/ default/files/fra_uploads/fra-2017-eu-mid- is-ii-main-results_en.pdf

26 Statewatch, 'Building the biometric state: Police powers and discrimination', February 2022, https://www.statewatch.org/publications/reports-and-books/building-the-biometric-state-police-powers-and-discrimination/

identification systems have been explicitly identified as a key tool to achieve this goal.[27] The fundamental right to non-discrimination and the principle of proportionality are therefore at great risk as race, ethnicity or skin colour is viewed as a proxy for an individual's migration status, and racialised people (regardless of nationality and EU citizenship status) are more likely to be exposed to racial profiling practices.[28] The European Commission itself has acknowledged that the new measures could "increase the risk" of "racial profiling and discriminatory selection of the persons being checked with the border areas".[29]

Use-cases of AI systems used for biometric identification

- **Mobile fingerprints in the UK** - Between 2019-2020, the *Racial Justice Network* and *Yorkshire Resists*, in conjunction with Queen Mary University of London, conducted research on the use and impacts of handheld fingerprint scanners for migration identity checks. The research shows the 'systematic racial bias' in the use of these systems and found that: "For every White North European person stopped and scanned in every 10,000 people, 48 Arabic people are scanned on average across the police jurisdictions. 14 Black residents are scanned for every White North European, 14 Asian people, almost 4 Chinese people or 2 South East Asian people for every White North European."
  '*STOP THE SCAN: Police use of mobile fingerprinting technology for immigration enforcement', Racial Justice Network, 6 March 2021, https://racialjusticenetwork.co.uk/2021/06/03/police-scanning-report/*
- **Smart Policing program in Greece**: In 2019, the Greek Interior Ministry launched the 'smart policing' program, which will allow police to receive smart devices with integrated software to enable them to scan vehicle license plates, collect fingerprints, and scan faces. The biometric data can be checked against around 20 databases, containing data both at the national and international levels. Following a complaint from the human rights organisation *Homo Digitalis*, the Hellenic Data Protection Authority launched an investigation into the legality of the program.
  Greece: New Biometrics Policing Program Undermines Rights', Human Rights Watch, https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights
- **IPERION system in Greece**: The IPERION system will be the asylum seekers' management system with regard to all the needs of the Reception and Identification Services. It will include a detailed record of the data of asylum seekers and will be responsible for access control (entry – exit via security turnstiles), by showing an individual card of a migrant, NGO member, worker and simultaneous use of fingerprints), the monitoring of benefits per asylum seeker using an individual card (food, clothing supplies, etc.) and the movements between the centres, KIDNs and Accommodation Facilities. Given the fundamental rights concerns, the Greek DPA recently launched an investigation into the deployment of the the Centaur system

---

27 Among the objectives of the Interoperability framework "assist in the process of identifying and returning any person who may not or no longer fulfil the conditions for entry to, stay or residence in the Member States", see Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, COM(2018) 302 final, 16 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

28 Ibid.

29 European Commission, 'Impact assessment report accompanying the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 on a Union Code on the rules governing the movement of persons across borders', 14 December 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52021SC0462&from=EN

by the Ministry of the Interior.
Homo Digitalis, "A major success for civil society in Greece: The Hellenic DPA launches an investigation into the Ministry of Immigration and Asylum re the YPERION and KENTAYROS IT systems" (9 March 2022), online: <https://www.homodigitalis.gr/en/posts/11024>

Considering the risks that these systems pose to fundamental rights, AI-enabled systems that perform biometric identification should be addressed by this Regulation and the relevant safeguards shall be applied to these uses. [30]

AI systems used in migration enforcement to conduct biometric identification should be classified as 'high-risk' and the following provision should be added in Annex III**.**

(5.B) Prohibit Remote Biometric Identification in publicly accessible spaces

Remote Biometric Identification (RBI) systems work by making a comparison between a person in a surveillance feed (via a biometric template) against a reference database / watch-list, to see if there is a match. The use of RBI in publicly accessible spaces refers to the location in which people being surveilled may or will have their biometric data captured or processed. [31]RBI systems have already been deployed in areas considered to be frequently attended by people with an irregular migration status, with the twofold, and unrelated, purposes of reducing irregular migration and improving security measures.

[30] See separate paper, entitled: Introduce obligations on users of high-risk AI systems, drafted by EDRi.
[31] See separate paper, entitled: Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces, drafted by European Digital Rights (EDRi), Access Now, ARTICLE19, Bits of Freedom, the Chaos Computer Club (CCC), Digitale Gesellschaft CH and the IT-Political Association of Denmark (IT-Pol).

Prohibited use-cases of AI systems used for biometric identification

- **SARI Real-Time:** In 2017, the Italian Interior Ministry acquired the *SARI Real-Time*, a facial recognition system capable of performing remote biometric identification. The plan was to use it as a "tactical system to monitor disembarkation operations and the various types of related illegal activities, filming them and identifying the people involved". In 2021, the Italian DPA deemed the deployment of SARI Real-Time unlawful, as the system lacked a legal basis for automatic processing of facial images, and it constituted a form of indiscriminate, mass surveillance.
  Statewatch, 'Italy: Interior ministry's facial recognition system is unlawful', 21 April 2021, https://www.statewatch.org/news/2021/april/italy-interior-ministry-s-facial-recognition-system-is-unlawful
  Garante per la Protezione dei Dati Personali, 'Parere sul sistema Sari Real Time' 25 March 2021, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9575877
- **RBI to counter irregular migration in Como** - In 2019, the municipality of Como (Italy) installed six cameras equipped with RBI systems in an area close to the city's railway station. The installation of this RBI system was the latest in a series of security measures that the city government had taken in response to the arrival of hundreds of people who found shelter in the city park after being stopped at the Italian-Swiss border. According to the city's Municipal Police, these events ''created inevitable degradation problems and spread a sense of insecurity among citizens"; consequently RBI systems were installed in areas believed to be frequented by people with an irregular migration status.
  In 2020, the Italian DPA issued a decision against the Municipality of Como mandating the suspension of the RBI system. According to the DPA, the processing of biometric data carried out by the Municipality of Como was unlawful.
  Privacy International, 'How facial recognition is spreading in Italy: the case of Como', 17 September 2020, https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como

RBI systems in publicly accessible spaces pose an unacceptable threat to fundamental rights to privacy, data protection, equality, non-discrimination, freedom of expression and information, peaceful assembly and association, liberty, dignity, and the presumption of innocence, as well as to basic principles of democracy, media freedom and the rule of law.[32]For this reason, the call for a prohibition of RBI systems in public accessible spaces as outlined in the civil society issue paper 'Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces' applies also to those systems deployed in the context of migration enforcement.[33]

(5.C) Prohibit remote biometric categorisation in publicly accessible spaces, and any discriminatory biometric categorisation

Biometric categorisation refers to the categorisation of individuals or groups on the basis of data about their bodies and behaviours. Systems also exist that claim to infer complex and sensitive attributes such as

[32] Ibid.
[33] Ibid.

political orientation, sexual orientation, and even 'criminality' on the basis of data about people's facial structure or biological characteristics. [34]

In the migration context, these systems can be used throughout various migration procedures, with the purpose of assisting migration authorities in assessing the credibility of the applicant's claim, as is the case of dialect recognition systems (see box, below).

Prohibited use case of Biometric Categorisation for the assessment of evidence in migration claims

- In 2017, the German Federal Office for Migration and Refugees (BAMF) introduced a **dialect recognition system** (DIAS) for the examination of asylum applications. The dialect recognition systems were introduced with the purpose of assisting the asylum authorities to assess the veracity of the applicant's claims regarding their origins. The dialect recognition system records a two-minute voice recording of the person describing a picture in their mother tongue; it then processes the voice data and calculates as a percentage how close the speech comes to a certain dialect. Evidence has shown that in some cases DIAS tools were used to take the final decision on an asylum application, despite the technical flaws and the intrinsic bias of these systems.
  Algorithm Watch, 'Automating Society: Germany',(2020)
  https://automatingsociety.algorithmwatch.org/report2020/germany/
  Vice, 'Eine Software des BAMF bringt Menschen in Gefahr', 20 August 2018,
  https://www.vice.com/de/article/a3q8wj/fluechtlinge-bamf-sprachanalyse-software-entscheidet-asyl?utm_campaign=28-01-22,%20Automated%20Society%22%20NL,%20EN&utm_medium=email&utm_source=Mailjet

The use of AI systems to infer sensitive or protected attributes of natural persons represents an extreme threat to fundamental rights, and violates the essence of our right to equality and non-discrimination. The proposed prohibition fulfills the aim of the recommendation from the EDPS-EDPB Joint Opinion that ""biometric categorisation" should be prohibited under Article 5".[35]

For this reason, the call for a prohibition of biometric categorisation systems in publicly accessible spaces as outlined in the civil society issue paper 'Prohibit remote biometric categorisation in publicly accessible spaces, and any discriminatory biometric categorisation' applies also to those systems deployed in the context of migration enforcement. [36]

6. AI systems in border control for monitoring and surveillance for the purpose of detection

[34] See separate paper, entitled: ***Prohibit remote biometric categorisation in publicly accessible spaces, and any discriminatory biometric categorisation***, drafted by by Access Now, European Digital Rights (EDRi), Bits of Freedom, ARTICLE19 and IT-Pol.

[35] EDPB-EDPS, Joint Opinion 5/2021, pag. 13, https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

[36] See separate paper, entitled: ***Prohibit remote biometric categorisation in publicly accessible spaces, and any discriminatory biometric categorisation***, drafted by by Access Now, European Digital Rights (EDRi), Bits of Freedom, ARTICLE19 and IT-Pol.

(6) Add to Annex III AI systems used in border control and management for monitoring and surveillance for the purpose of detection

AI systems are increasingly used in the migration context for generalised and indiscriminate surveillance at borders, including for the detection and recognition of human beings, both at land and at sea. They include the deployment of various AI-based technologies, including augmented reality (AR) systems, unpiloted vehicles and devices, intelligent detection platform and AI-assisted sensors.

Use-cases of AI systems used in border control and management for the purpose of detection

- **RoBorder:** The intention of this research project is to "implement a heterogenous robot system and enhance it with detection capabilities for early identification of criminal activities at border and coastal areas along with marine pollution events". The system encompasses an AI-enabled **swarm of heterogenous robots for border surveillance**, including aerial, surface, underwater and ground vehicles as well as data fusion and processing, object detection and decision-support capabilities.
- **FOLDOUT**: The aim of FOLDOUT is to build a system which combines various sensors and technologies and fuses them into a **through-foliage detection platform for border surveillance**. The goals are the detection of irregular border crossings in forest terrain, improving border surveillance and the detection of illegal transport and entry of goods. AI-assisted sensors allow the system to perceive, localise, track and classify objects into humans, vehicles and other objects.
- **BorderUAS:** The project aims at developing a **semi-autonomous border surveillance platform combining unmanned aerial vehicles with ultra-high-resolution multi-sensor surveillance payload**. It will use the ground-based infrastructure of border police units (command & control centres) and data models to identify irregular crossing patterns and preferred routes and advanced audio/video analytics to provide additional detection capabilities.
- **iBorderCtrl:** It includes the **Hidden Human Detection Tool** (HHD), which supports the Border Guard in detecting any hidden people inside various vehicles (i.e. passengers attempting illegal border crossing). The functionality provided allows detection of humans hidden within vehicles such as cars or closed compartments (containers carried on trucks or train wagons).
- **ARESIBO (Augmented Reality Enriched Situation awareness for Border security)**: It aims at improving the efficiency of the border surveillance systems by providing the operational teams and the tactical command and control level with accurate and comprehensive information. It includes the use of **Augmented Reality techniques** to elaborate and provide to the operators a situation awareness picture which is fit for their missions
- **Centaur**: This partly-automated surveillance system operates in the refugee reception centres on the islands of Lesbos, Chios, Samos, Leros, and Kos. The system includes AI-assisted drones that perform movement analysis, suspicious crowds and incidents systems and automated threat detection tools.
- **Frontex**: The European Border and Coast Guard Agency has also been developing pilot projects utilizing AI-based capabilities in the maritime domain and overall situational awareness, using real-time trend forecasting for motion detection, object monitoring, and threat forecasting.

This paper was drafted by Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch. It is supported by the European Centre for non-profit Law (ECNL), European Disability Forum (EDF), Privacy International. It follows the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.

Such systems pose numerous risks and potential adverse effects on fundamental rights, raising the serious concern that they are not currently categorised as 'high-risk' systems under the AIA.

The fundamental rights concerns with such systems largely relate to the context in which they are used. In particular, insofar as such systems are used to 'detect' human presence for the purpose of 'combating irregular migration', there is a serious concern that such systems can facilitate illegal interdiction, exacerbate violence at border crossings and racial profiling, and other forms of discrimination.

Insofar as the use of AI-based surveillance systems, even those that do not identify individuals, may pinpoint areas or commonly used migratory routes, there is a risk that such systems could be used for the purpose of interdiction and the prevention of irregular border crossings, thus forcing people to risk using more unsafe routes, increase the risk of injury and death as well as the use of smugglers to make their migration journeys. [37] Such systems serve as the apparatus for the ongoing criminalisation of migration and people on the move, increasing their risk of harm- with limited opportunity for recourse or accountability.

They therefore risk unnecessary and disproportionate interference with several following fundamental rights enshrined in the EU Charter of Fundamental Rights and also protected under international human rights law, such as the right to human dignity, the right to asylum, the prohibition of torture and inhuman or degrading treatment or punishment, the right to liberty and security, the protection in the event of removal, expulsion or extradition, the rights of the child and the right to an effective remedy.

More structurally, the development, testing, funding and deployment of AI systems for generalised surveillance of border areas raises a substantial concern of mass surveillance.

Given the elevated risk of violation of fundamental rights and broader structural injustices, all AI systems that are part of a border control system should be addressed within the scope of this Regulation. This would guarantee that all obligations under the AIA to ensure accountability and transparency of uses of AI (including for example, to include a fundamental rights impact assessment for uses of high-risk AI) would therefore apply to these use cases.[38]

7. Assessment of evidence in migration claims

AI systems aimed at assessing the authenticity and veracity of evidence can utilise intrusive techniques with significant fundamental rights implications.

Increased oversight is required for AI systems used in the assessment of evidence in migration claims. Often, there are significant issues with respect to accuracy as these systems are not particularly suited to grasp nuanced cultural and linguistic differences, especially in non-dominant languages and cultures. The level of intrusiveness of some AI systems raise serious concerns with their compatibility with fundamental rights and the EU legislation on data protection.

---

37 EDRi (2020). 'Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up', authored by Petra Molnar.

38 See separate paper, entitled: 'Introduce obligations on users of high-risk AI systems', drafted by EDRi.

Use-cases: AI systems used for the assessment of evidence in migration claims

- Since 2017, the **German Federal Office for Migration and Refugees (BAMF)** introduced **data carrier evaluation** in the context of asylum applications, should the applicant not be able to present valid passports or passport replacement documents. The evaluation allows for the extraction and analysis of data from data carriers such as phones in order to check the stated origin and identity of the applicant. [39]
  The human rights organisation Gesellschaft für Freiheitsrechte e.V. challenged the practice before several German administrative courts and questioned its compatibility with EU legislation on data protection and privacy. In June 2021, a Berlin court ruled in the first of the three cases that searching the phone belonging to an asylum-seeker from Afghanistan was unlawful.
  Gesellschaft für Freiheitsrechte e.V, "Invading Refugees' Phones: Digital Forms of Migration Control", (2020) https://freiheitsrechte.org/study-invading-refugees-phones/

- In March 2022, **'the UK High Court ruled that the Home Secretary acted unlawfully and breached human rights and data protection laws** by operating a secret, blanket policy of seizing, retaining and extracting data from the mobile phones of asylum seekers arriving by small boat'.
  See Privacy International's press release: 'High Court rules seizing and retaining mobile phones from asylum seekers unlawful',
  https://www.privacyinternational.org/press-release/4812/press-release-high-court-rules-seizing-and-retaining-mobile-phones-asylum

Further, when misapplied or resulting in inaccuracies, such systems impact the fundamental right to seek protection and to avail oneself of fair asylum procedures, rights afforded under the UN Refugee Convention and its accompanying Protocol, the EU Qualification Directive (2011/95), and natural justice principles such as the right to a fair procedure, access to transparent mechanisms of redress and other administrative rights. These legal frameworks do not require the use of intrusive methods in the assessment of the veracity of the documentation brought in support of the claim.

(7) Ensure AI for the assessment of evidence in migration claims is included in Annex III

Article 7.d. of Annex III should be amended in order to explicitly include the use of systems that seek to assess veracity of any evidence brought in support of the claim, such as dialect detection and mobile data extraction tools. In order to guard against the likely harms stemming from the use of such intrusive systems, Art 7(d) of Annex III should be amended.

[39] GFF, "Invading Refugees' Phones: Digital Forms of Migration Control" (2019), https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf

8. Ensure AI as part of large-scale EU IT databases are within scope of the Artificial Intelligence Act

Article 83 of the AIA excludes from the scope of the Regulation AI systems that are components of large-scale IT systems listed in Annex IX, namely those in areas of freedom, security and justice. In particular, this exemption from scope applies to AI systems that are a component of large scale EU migration databases, including: the Schengen Information System, the Visa Information System, Eurodac, the Entry/Exit System, the European Travel Information and Authorisation System (ETIAS), the European criminal records information system on third-country nationals (ECRIS-TCN)Is, and the Interoperability framework.

All of these large-scale IT systems involve or intend to involve the automated processing of personal and sensitive data, risk assessment systems and the use of technology for biometric identification, authentication and verification.[40] As such, most of these systems will involve the use of AI systems which have been defined as posing a high risk to rights and safety as defined in Article 6(2) and that are already included in the scope of Annex III, but will nevertheless be exempted from the associated rules. This wide exemption in the scope of the Act is harmful for three main reasons:

Large numbers of people affected by EU IT databases

The large-scale IT systems at stake would affect almost every third-country national that has any administrative or law enforcement link to the European Union. Such systems not only process data for the purpose of profiling or decision-making in relation to international protection or visa claims, but also in some instances facilitate law enforcement access to data. Excluding AI systems that are components of such systems from the scope of the Act therefore means that the safeguards outlined in the Regulation would not apply to hundreds of millions of people, with potentially serious consequences for fundamental rights.

Severe fundamental rights implications and societal risks

The exclusion from scope of AI systems that are components of large-scale AI systems would mean that the safeguards included in the AIA do not apply to systems in the context of EU migration databases.[41]

In many cases, such systems impact fundamental rights to privacy and data protection, the right to asylum, non-discrimination, and others as outlined in the previous sections of this paper. Further, due to the wide-ranging mandate of EU IT databases and numbers of third-country nationals affected, there are substantial concerns that such practices may comprise disproportionate infringements of data protection rights and amount to mass surveillance.

---

40 European Commission, "Opportunities and challenges for the use of artificial intelligence in border control, migration and security . Volume 1, Main report" (2020), https://op.europa.eu/en/publication-detail/-/publication/c8823cd1-a152-11ea-9d2d-01aa75ed71a1/language-en

41 Niovi Vavoula, 'Unpacking the EU proposal for an AI Act: implications for AI systems used in the context of migration, asylum and border control management', Turkish Policy Quarterly (4 March 2022), http://turkishpolicy.com/article/1100/unpacking-the-eu-proposal-for-an-ai-act-implications-for-ai-systems-used-in-the-context-of-migration-asylum-and-border-control-management

Through Article 83, the European Commission attempts to set a dangerous precedent in the area of Artificial Intelligence, such that any system used in activities for the purported furthering of national and public security can be excluded by the scope of this Regulation, without evidence or impact assessments, and in spite of its own recognition of the heightened risk to health and fundamental rights they present.

Undermining credibility of the Regulation

The exemptions proposed in Article 83 risks undermining the credibility of the whole Regulation, if maintained. With Article 83, the European Commission is implicitly admitting either that these systems would not be able to comply with the obligations and safeguards outlined in the Regulation, or that the EU simply should not be subject to scrutiny or oversight as a provider and user of high-risk AI. Further, this provision reinforces the notion of a differential approach to fundamental rights when migration is the subject matter and people on the move are the right-holders.

Therefore, article 83 should be amended to explicitly include within scope of the act AI systems as components of Large scale IT systems.

This paper was drafted by Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch. It is supported by the European Centre for non-profit Law (ECNL), European Disability Forum (EDF), Privacy International. It follows the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.