UNPACKING THE EU PROPOSAL FOR AN AI ACT: IMPLICATIONS FOR AI SYSTEMS USED IN THE CONTEXT OF MIGRATION, ASYLUM AND BORDER CONTROL MANAGEMENT

On 21 April 2021, the European Commission presented its long-awaited proposal for a Regulation laying down harmonized rules on AI.[**] The proposal, which is based on Articles 16 and 114 of the TFEU on data protection and the internal market respectively, aims at a risk-based approach that respects EU values and protects personal data and fundamental rights at the same time. This contribution aims to critically examine which AI tools fall within the scope of AI Act, how these are classified and whether the proposed approach poses concerns for the protection of fundamental rights. To that end, the next section provides a snapshot of the proposal to inform the subsequent analysis, followed by an analysis on which migration-related AI systems aiming to identify potential loopholes. In addition to an appraisal of which AI systems are envisaged within the scope of the proposal, this article assesses Article 83 of the proposal, which excludes several AI initiatives from its scope.

Niovi Vavoula*

TPQ
Winter 2021/22

* Dr. Niovi Vavoula is a lecturer in Migration and Security at University of London.
**Commission, Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (Proposal for AI Act) COM (2021) 206 final.

Overview of the Proposal for an AI Act

The proposed Regulation distinguishes AI systems on the basis of the risk they pose to the fundamental rights of individuals or EU values. In light of this, according to Article 5 of the proposal, particularly harmful AI practices should be prohibited, such as those that can manipulate vulnerable individuals through subliminal techniques. These practices may cause harm to the manipulated individual or others. For the purpose of law enforcement, social scoring and real-time remote biometric identification are not permitted in publicly accessible areas due to the 'unacceptable risk' they create.[1] 'High risk' AI systems impact people's safety or fundamental rights, and are therefore considered high-risk. Systems listed in Annex III include those used for biometric identification and categorisation of individuals, critical infrastructures (such as transportation), formal education or vocational training, essential private and public services (such as credit scoring which denies citizens a loan), law enforcement, migration, asylum, border control, management and administration of justice and democratic processes. The deployment of 'high-risk AI' systems will need to undergo a conformity assessment before being placed on the market and comply with a range of safety requirements (regarding, for instance, risk management, human oversight and data governance).[2] In addition, an *ex-post* market surveillance and supervision must be put in place to ensure compliance with the obligations and requirements for all high-risk AI systems already placed on the market.[3]

Zooming into Migration, Asylum and Border Control Management

Under migration, asylum and border management, Annex III details four different types of AI systems. These are:

(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; and

[1] For criticism about the see Center for Artificial Intelligence and Digital Policy, *Center for AI & Digital Policy (CAIDP) Statement on Proposed EU AI Regulation* (28 July 2021).

[2] Center for Artificial Intelligence and Digital Policy, (2021), Chapter 2 and Article 43.

[3] Center for Artificial Intelligence and Digital Policy, (2021), Article 61.

(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.

"Similarly, data provided by short or long-stay visa and residence permits applicants will be subject to comparable rules, except that the automated processing will never lead to automatic issuance of a visa or a residence permit and there is always manual processing of the application by visa authorities."

The first type essentially refers to emotion recognition systems that claim to infer people's emotions and mental states from physical, physiological, behavioural, as well as biometric data. Their use worldwide is currently in its early stages, but not prohibited. In the U.S, the Department of Homeland Security funded research of the virtual border agent technology known as the Automated Virtual Agent for Truth Assessments in Real-Time (AVATAR) and allowed it to be tested it at the U.S-Mexico border on travelers who volunteered to participate.[4] Perhaps the most prominent application of emotion recognition in the EU was Frontex's highly contentious iBorderCtrl project (Intelligent Portable Border Control System) from September 2016 through August 2019. Detecting mental states and emotions by examining a person's facial expressions as well as other physiognomic indicators has attracted considerable attention. Hungary, Latvia, and Greece piloted an automated lie-detection test analysing facial micro-gestures at three undisclosed airports in order to identify 'biomarkers of deceit'.[5] By scanning refugees' and migrants' facial expressions as they answer questions, the machine is able to determine whether they have lied to the machine, and then pass on that information to border officers. The project has been challenged before the CJEU on transparency grounds. MEP Patrick Breyer has requested that the EU Research Agency (REA) release classified documents evaluating the 4.5 million euro trial of AI lie detectors to bolster EU border control to determine its ethical and legal justifiability, as well as the results of the technology, on the ethical justification and legal admissibility.[6] In December 2021, the General Court of Justice opined that REA may no longer keep these documents

[4] Jeff Daniel, "Lie-detecting Computer Kiosks Equipped with Artificial Intelligence look like the Future of Border Security," *CNBC*, 15 May 2018, https://www.cnbc.com/2018/05/15/lie-detectors-with-artificial-intelligence-are-future-of-border-security.html accessed on 25 February 2022.

[5] Javier Sánchez-Monedero and Lina Dencik, "The Politics of Deceptive Borders: 'Biomarkers of Deceit', and the Case of iBorderCtrl," *Information, Communication & Society*, Vol 1 (2020).

[6] Zach Campbell, Caitlin L Chandler and Chris Jones, "Sci-fi Surveillance: Europe's Secretive Push into Biometric Technology," *The Guardian*, 10 December 2020, https://www.theguardian.com/world/2020/dec/10/sci-fi-surveillance-europes-secretive-push-into-biometric-technology accessed on 25 February 2022.

completely secret. The ethical and legal evaluation of technologies for 'automated deception detection' or automated risk assessment must be published, as long as they do not relate specifically to the iBorderCtrl project.[7] Nevertheless, to protect commercial interests, the examination of ethical risks (e.g. stigmatization and false positives) and legal admissibility of the concrete technology of iBorderCtrl, as well as reports of project results, may be kept confidential.

Considering that the EU has already been testing AI polygraphs and lie detectors for years, it is unsurprising that the proposal does not wish to ban them entirely. This is notwithstanding the fact that the programme has reported an accuracy rate of 73-75 percent and has raised (well-deserved) criticism about its validity that its applicability in a real-life context.[8] Similarly, the U.S. AVATAR as a deception-detection judge has a success rate of 60 to 75 percent and sometimes up to 80 percent.[9] Expressions and facial expressions differ greatly between cultures and situations. As a result, emotion detection has limited reliability;[10] emotion categories are neither reliably expressed through, nor unequivocally associated with a common set of facial movements. Furthermore, facial expressions do not perfectly match emotion categories, so generalizability is generally limited. In addition, the effectiveness of such tools has yet to be proved, whereas the risk of racial profiling is significant.[11] From that perspective, the judgment by the General Court is somewhat disappointing, as the results of the project could support the claim that emotion detection systems posed such ethical and fundamental rights challenges to the extent that they should not be classified as high risk and should be banned altogether, as advocated by civil society actors.[12] At least, it is obligatory for project participants to make a scientific publication about the project within four years and therefore it is possible to get more answers on the project.

Whenever automated assessments are made as to whether an individual may pose a security, immigration, or health risk, these are rightly classified as high-risk AI

[7] Case T-158/19 *Patrick Breyer v European Research Executive Agency*, (2021), ECLI:EU:T:2021:902.

[8] Javier Sánchez-Monedero and Lina Dencik, (2020).

[9] Daniel, 15 May 2018.

[10] It has even been called as 'pseudoscience' because the 'micro-expressions' the software analyses cannot be reliably used to judge whether someone is lying. In 2019 The Intercept tested the iBorderCtrl system. The video lie detector falsely accused its reporter of lying — judging she had given four false answers out of 16, and giving her an overall score of 48, which it reported that a policeman who assessed the results said triggered a suggestion from the system she should be subject to further checks (though was not as the system was never run for real during border tests). See Ryan Gallagher and Ludovica Jona, "We Tested Europe's New Lie Detector for Travelers – And Immediately Triggered a False Positive," *The Intercept*, 26 July 2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/ accessed on 25 February 2022.

[11] American Civil Liberties Union (ACLU), *Bad Trip: Debunking the TSA's 'Behavior Detection' Program* (2017).

[12] "An EU Artificial Intelligence Act for Fundamental Rights a Civil Society Statement," *Accessnow*, 30 November 2021, https://www.accessnow.org/cms/assets/uploads/2021/11/joint-statement-EU-AIA.pdf accessed on 25 February 2022.

"Chatbots use natural language processing to conduct human-like conversations with users and they have been criticised for embedding biases and using discriminatory language. Therefore, these should also be considered as high risk."

systems. A subset of automatic assessments falls under this category of AI, which incorporate algorithmic profiling against risk indicators developed through statistical analysis of rates of overstaying and refusals of entry. It also includes the use of AI tools to identify irregular traveling patterns as an additional piece of risk analysis and identify so-called 'mala fide' travelers. This category also includes AI systems that determine whether an asylum seeker poses a risk of absconding and should therefore be detained. The EU legislature has already adopted legal instruments that will require in the near future such automated assessments in the cases of the European Travel Information and Authorisation System (ETIAS)[13] and the Visa Information System (VIS).[14] Visa-free nationals will have to register for ETIAS online in order to provide a wide array of personal data, which will then be cross-checked against databases, both European and some Interpol ones, according to specific screening rules, in order to enable profiling on the basis of risk indicators. An ETIAS authorization will be automatically provided in the event that there is no problem with the data provided, otherwise the application will go through manual processing by the responsible Member State. Similarly, data provided by short or long-stay visa and residence permits applicants will be subject to comparable rules, except that the automated processing will never lead to automatic issuance of a visa or a residence permit and there is always manual processing of the application by visa authorities.[15] As argued elsewhere, the risk of discrimination both direct and indirect in the design of the algorithms is particularly high. As they are trained using pre-existing data and past decisions, they run the risk of repeating all of the implicit and inherent biases of those earlier decisions. Such initiatives are already tried (unsuccessfully)

[13] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018: *Establishing a European Travel Information and Authorisation System (ETIAS) and Amending Regulations (EU) No 1077/2011*, (*EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226* [2018] OJ L236/1.

[14] Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 *Amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896* of the European Parliament and of the Council and repealing *Council Decisions 2004/512/EC and 2008/633/JHA*, for the purpose of reforming the Visa Information System [2021] OJ L248/11.

[15] For further information see Niovi Vavoula, "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*, Vol. 23, No. 4 (2021): p. 457.

in the UK, where the Home Secretary decided to withdraw an algorithm used to filter visa applications after being called out as racially discriminatory.[16] The system took some information provided by visa applicants and automatically processed it, giving each person a colour code based on a "traffic light" system - green, amber, or red. Similarly, in Canada the Government tested AI solutions to triage temporary resident visa applications.[17] Regrettably, these systems will not fall within the scope of the AI Act. According to article 83, AI systems which are components of large-scale IT systems governed by a series of EU legal instruments (listed in Annex IX) and implemented before 12 months after the application date of the AI Act - after its enactment - are excluded from the AI Act, unless the replacement or amendment of those legal acts results in a significant change to the design or intended purpose of the AI system or AI systems concerned. As ETIAS is slated for implementation in 2023, and the VIS rules will be in place not long after, it is almost certain that algorithmic profiling of travelers and migrants will fall outside the scope of the AI Act, which is still being negotiated and will take two years to enforce in the Member States. That said, the principle that automated risk assessments should be classified as high risk will still be applicable, but the deployment of AI systems in relation to these databases will not be subject to the safeguards encompassed in the forthcoming AI Act.[18]

The exclusion clause of Article 83 is particularly problematic for a series of other reasons. In addition to ETIAS and VIS, the remaining information systems that process personal data of third-country nationals, Schengen Information System (SIS), Eurodac, Entry/Exit System and European Criminal Record Information System for Third-Country Nationals (ECRIS-TCN) are also under development

[16] Henry McDonald, "Home Office to scrap 'racist algorithm' for UK visa applicants," *The Guardian*, 4 August 2020, https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racistalgorithm-for-uk-visa-applicants

[17] Petra Molnar and Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System," (2018); Lucia Nalbandian, "Using Machine-Learning to Triage Canada's Temporary Resident Visa Applications," (Working Paper 2021/09, July 2021).

[18] The requirements however prescribed in Opinion 1/15 and *La Quadrature du Net and Others* about automated analysis will still be applicable. In particular, according to Opinion 1/15, a) pre-established models and criteria (algorithms), should be 'specific and reliable' to individuals who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime and should be non-discriminatory; b) that the databases cross-checked must be reliable and up to date; c) any hit following the automated processing of that data must be subject to an individual re-examination by non-automated means; d) the pre-established models and criteria and the databases used are not discriminatory and are limited to that which is strictly necessary, the reliability and topicality of those pre-established models and criteria and databases used should, taking account of statistical data and results of international research. In *La Quadrature du Net and Others*, the Court of Justice of the EU added that the models or criteria to conduct an automated analysis cannot be based on sensitive data *in isolation.* Furthermore, the Court acknowledged the need to regularly re-examine the algorithms and the databases used to ensure that they are reliable, up-to-date and in practice non-discriminatory and limited to what is strictly necessary to achieve the intended purpose. Lastly, the Court held that because of the margin of error that may result from the automated analysis, there has to be an individual non-automated re-examination of a positive result before adopting a measure that may have adverse effect on the person concerned. See Opinion 1/15 ECLI:EU:C:2017:592; Joined Cases C511/18, C512/18 and C520/18 *La Quadrature du Net and Others v Premier Ministre and Others* ECLI:EU:C:2020:791.

(EES and ECRIS-TCN) or refurbishment (SIS and Eurodac) to encompass among others facial recognition technology, which enables biometric identification and is also considered as high risk type of AI systems. Consequently, Article 83 essentially excludes all information systems for third-country nationals from the protective scope of the AI Act. This exclusion applies unless those systems are subject to 'significant changes' in design or intended purpose. As mentioned in the Joint Opinion of the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB), the threshold for 'significant changes' is not clear. Recital 66 of the Proposal specifies a lower threshold for conformity re-assessment 'whenever a change occurs which may affect the compliance' and it has been rightly argued, a similar threshold would be appropriate for Article 83 as well, at least for high risk AI systems.[19] According to the Commission report on the opportunities and challenges for the use of AI in border control, migration and security, additional initiatives are underway, including application triaging, along the lines of the UK failed experiment. [20] In the case of ETIAS, the report notes that there will be in the future individual risk assessment by an AI tool to assist in manual processing.[21] These initiatives should be considered as 'significant changes' to the functioning of the systems to subject them to the forthcoming AI Act. Therefore, if these initiatives are to be adopted and implemented within the next few years, it makes no sense to keep the exclusion clause. Overall, it is unclear why this exclusion clause, which will create protection gaps, has been included in the first place. One possible explanation is the fact that the AI systems that will be included in the information systems for third-country nationals are already under development and awaiting for the adoption of the AI Act could potentially change the timeline for implementation as well as change the procedures for testing the algorithms that will be used, which are to be developed by the ETIAS Central Unit, within the European Border and Coast Guard. In any case, and as a *minimum*, considering that the entry into application is envisaged for 24 months following the entry into force of the future Regulation, exempting AI systems already placed on the market for an even longer period of time is not appropriate.[22] Moreover, while the Proposal also provides that the requirements of the Regulation shall be taken into account when evaluating each large-scale IT system as provided by the legal acts listed in Annex IX, both EDPB and EDPS believe that conditions for putting AI systems into service should be applicable from the date of application of the future Regulation. That said, Article 83 contains a protection clause; the requirements of the AI Act must be taken into

[19] EDPS and EDPB, *EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence* (Artificial Intelligence Act) (18 June 2021): p. 14.

[20] Commission, "Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security," (May 2020): p. 16.

[21] Commission, (May 2020): p. 19.

[22] EDPS and EDPB, (18 June 2021): p. 14.

account, where applicable, in the evaluation of large-scale IT systems. This is an important safeguard, but it must be noted that in the past, the legal bases of information systems have been amended before the conduct of an evaluation and therefore it is possible that the AI Act prescriptions will not be taken into account at that phase. Thus, it is imperative that the threshold of placing existing AI systems within the scope of the Act is lowered to minimize gaps in protection.

Under the third type of AI systems, AI systems might enable tools that detect forgeries of travel documents or other supporting documents. Furthermore, these systems are rightly regarded as high risk, since they are bound to significantly affect individuals if the results (false positives and negatives) are inaccurate. For example, various unjustified claims could be made against an individual (e.g., document fraud) on the basis of inaccurate underlying data. Meanwhile, individuals may face detention and degrading treatment when suspected of criminal conduct.

In regard to the last type of AI systems classified as high risk, the proposal refers to assistance in examining requests for asylum, visas, and residence permits, as well as complaints regarding eligibility of the natural person applying for such a status. AI systems of this type seem closely related to the second, but they may encompass broader initiatives such as personalized application forms that tailor questions to the applicant using AI. In this case, augmented application forms could be developed, or artificial intelligence systems could be used to perform vulnerability assessments of asylum seekers to determine if they need to be further investigated by a social worker or granted special procedural rights. The repercussions of severe decisions and actions in this context can have particularly severe consequences on individuals; the remedies to reverse the harm caused by these actions and decisions are unclear.

Finally, there are three further reasons why the list of migration-related AI systems is problematic. The first one concerns the lack of references to the use of AI systems for predictive analytics of migration.[23] As mentioned by Beduschi, AI technologies to foresee arrivals and prepare more efficiently for large influxes of people.[24] In February 2022, the Commission along with the European Union Asylum Agency (former European Asylum Support Office) announced the development of a forecasting model for asylum flows.[25] In addition, the use of chatbots and intelligent

[23] European Digital Rights (EDRi) and others, "An EU Artificial Intelligence Act for Fundamental Rights A Civil Society Statement," *Accessnow*, (30 November 2021). https://www.accessnow.org/cms/assets/uploads/2021/11/joint-statement-EU-AIA.pdf accessed 25 February 2022

[24] Ana Beduschi, "International Migration Management in the Age of Artificial Intelligence," *Migration Studies*, Vol. 9, No. 3 (2020): p. 576.

[25] Marcello Carammia, Stefano Maria Iacus and TeddyWilkin, "Forecasting Asylum-related Migration Flows with Machine Learning and Data at Scale," *Nature Scientific Reports* (2022). Prior to this, EASO developed an Early Warning and Forecasting System that allows for the prediction of migration movements, which used as a basis social media data, which was outside of its mandate and for which the agency was criticised.

agents, which would take in information, answer questions posed by the applicant, and ensure data quality, also falls outside the scope of the AI Act. Chatbots use natural language processing to conduct human-like conversations with users and they have been criticized for embedding biases and using discriminatory language.[26] Therefore, these should also be considered as high risk. Furthermore, individuals should know in advance whether they are dealing with a human or a machine. Finally, the proposal refers to AI systems used by public authorities only, whereas increasingly there are instances of border management entrusted to private companies, for example, in the management of camps in the Greek islands.[27] Due to the blurred lines between public and private security it was imperative that the use of AI system for immigration control purposes would fall within the scope of the AI Act regardless of the actor involved. In fact, the latest Council documents consolidating the amendments proposed during the Slovenian presidency address this concern.[28]

This contribution pointed out that the proposed EU AI Act categorizes as high risk several AI systems that may be used for immigration-related purposes; however, there are significant flaws in the current approach, which the Council has only partially rectified. Negotiations are still ongoing, so it will be up to the Parliament to push for a better balance between taking advantage of the opportunities offered by AI and protecting fundamental rights.

[26] Christopher Heine, "Microsoft's Chatbot 'Tay' Just Went on a Racist, Misogynistic, Anti-Semitic Tirade," *AdWeek*, 24 March 2016, https://www.adweek.com/performance-marketing/microsofts-chatbot-tay-just-went-racist-misogynistic-anti-semitic-tirade-170400/ accessed on 25 February 2022.

[27] "Concerns over States contracting Private Security Companies in Migration Situations," (United Nations High Commissioner for Human Rights, (20 December 2019). https://www.ohchr.org/EN/NewsEvents/Pages/SecurityPrivatisationMigrationContexts.aspx accessed on 25 February 2022.

[28] Council, *Document 14278/21* (29 November 2021).