Co-funded by the
Erasmus+ Programme
of the European Union

Jean Monnet Network on EU Law Enforcement

Working Paper Series

DRAFT – DO NOT CITE

Enforcing Migration, Asylum and Border Management Policies through AI-based Tools: What Role for the AFSJ Agencies?

Niovi Vavoula[1]

Abstract

Since the past few years, the exponential increase in computational power coupled with the availability of large quantities of data has heightened the interest for Artificial Intelligence (AI). In the field of international migration in particular, AI has the potential to revolutionise the way states manage immigration by modernising border controls, as well as expediting decision-making in relation to visa residence permits or asylum applications. At EU level, efforts to incorporate and regulate AI systems in immigration control are already underway, but the proposed AI Act, which aims to horizontally regulate AI systems, to a large extent excludes from its scope AI systems already under development. In this regard, much less attention has been paid to the role of agencies in enforcing migration, asylum and border management policies through the design, testing and deployment of AI-based solutions. Indeed, the main four EU agencies operational in the AFSJ are already engaged with AI-related activities, based on increased data collection; Europol's mandate has been recently updated to enable the agency to process data for research and innovation purposes. Furthermore, Frontex has also been heavily invested in identifying Ai-based solutions for the border management of the EU external borders. The European Asylum Support Office (EASO), renamed as European Union Asylum Agency (EUAA), has also been at the forefront, not least because of its endeavours to forecast migratory flows outside of its mandate. As for eu-LISA, its technical nature has enabled this agency to test and promote a high-tech agenda for future deployment of AI-based tools, including facial recognition technology.

This contribution aims to take stock of the current state of play in connection with the work of agencies in this field and highlight the potential benefits and challenges posed by the involvement of EU AFSJ agencies in the design and deployment of AI tools for immigration related purposes, in terms of fundamental rights, but also in terms of rule of law. It argues that the move towards AI has provided a first-class opportunity for agencies to increase their mandate *de jure* or *de facto*. Agencies have got their hands on more personal data without corresponding safeguards for the protection of fundamental rights or being accompanied with sufficient transparency and accountability mechanisms. The potential effectiveness of these tools will also be considered. The contribution will point out the legal gaps and provide recommendations for future regulation.

Keywords:

Agencies, Europol, EBCG, EUAA, eu-LISA, Artficial Intelligence

[1] Short biography of the author may be inserted here

I. Introduction

The exponential increase in computational power coupled with the availability of large quantities of data has heightened the interest for Artificial Intelligence (AI). In the field of international migration in particular, AI has the potential to revolutionise the way states manage immigration by modernising border controls, enhancing the ability to govern border spaces, expediting decision-making in relation to visa residence permits or asylum applications and overall control population movements. The underlying rationale focuses on the apparent advantages of increased efficiency, improved preparedness and enhanced border security.[2] Specific applications are numerous, ranging from predicting migration, automated decision-making and AI-based lie detectors using emotion recognition, all of which are regulated to a limited extent only (due to their very recent application)[3] and encroach on fundamental rights of foreigners.

At EU level, efforts to incorporate and regulate AI systems in immigration control are already underway, but the proposed AI Act, which aims to horizontally regulate AI systems, to a large extent excludes from its scope AI systems already under development.[4] Much less attention has been paid to the role of agencies in enforcing migration, asylum and border management policies through the design, testing and deployment of AI-based solutions. Indeed, the main four EU agencies operational in the AFSJ are already engaged with AI-related activities, based on increased data collection; Europol's mandate has been recently updated to enable the agency to process data for research and innovation purposes. Furthermore, Frontex has also been heavily invested in identifying Ai-based solutions for the border management of the EU external borders. The European Asylum Support Office (EASO), renamed as European Union Asylum Agency (EUAA), has also been at the forefront, not least because of its endeavours to forecast migratory flows outside of its mandate. As for eu-LISA, its technical nature has enabled this agency to test and promote a high-tech agenda for future deployment of AI-based tools, including facial recognition technology.

This article aims to take stoczk of the current state of play in connection with the work of agencies individually and in collaboration in this field and highlight the potential benefits and challenges posed by the involvement of EU AFSJ agencies in the design and deployment of AI tools for immigration related purposes, in terms of fundamental rights, but also in terms of rule of law. It argues that the move towards AI has provided a first-class opportunity for agencies to increase their mandate *de jure* or *de facto*. Agencies have got or will get their hands on more personal data without corresponding safeguards for the protection of fundamental rights or being accompanied with sufficient transparency and accountability mechanisms. The potential effectiveness of these tools will also be considered. The contribution will point out the legal gaps and provide recommendations for future regulation.

II. Europol

Headquartered in The Hague since 1999, Europol is tasked with supporting and strengthening cooperation between EU Member States in the area of cross-border police cooperation. The agency primarily operates as an every growing 'information hub', collecting and further processing information deriving from Member States

[2] Tuba Bircan and Emre Eren Korkmaz, 'Big data for whose sake? Governing migration through artificial intelligence' (2021) *Humanities & Social Sciences Communications*.

[3] One of the first AI applications was initiated in 2007 by the Hong Kong Immigration Department as a part of the eBrain project. The agency employed a suite of AI technologies to streamline administrative tasks like visa applications and processing travel documents, identity cards, and work permits. In mid-2017, the United Nations initiated the Unite Ideas Internal Displacement Event Tagging and Extraction Clustering Tool challenge. The winner was the Data for Democracy team, which built a tool capable of tracking and analysing refugees and other people forced to flee or evacuate their homes.

[4] 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' COM(2021) 206 final. For an analysis see Niovi Vavoula,

and increasingly from third countries and private parties.[5] Though primarily a law enforcement agency, Europol is progressively engaged in processing personal data in the context of border management, also for the identification of migrants and in cross-border anti-migrant (smuggling) operations.[6]

In December 2020, the Commission tabled a proposal on the reform of Europol's mandate[7] proposing among others a key role for Europol in research and innovation so as to support Member States to battle the challenges of criminal exploitation of advanced technologies, such as encryption.[8] The revised text was adopted on 24th May and the new Europol Regulation is expected to be published by the end of June.[9]

Already since October 2019, the Justice and Home Affairs (JHA) Council called for 'the creation of an innovation lab at Europol which could act as an observatory for the creation of new technological developments and drive innovation, including by developing common technological solutions for member states in the field of internal security'.[10] Similarly, the European Parliament in its Resolution of December 2018 called 'for the active involvement of EU agencies such as Europol and CEPOL in EU security research projects'.[11] However, even though Europol has established the Innovation Lab[12] aimed at supporting investigators and law enforcement agencies in making the most of emerging technologies, Europol does not have a mandate to support Member States in fighting serious crime and terrorism by fostering research and innovation and using the results of research relevant for law enforcement, including safeguards with respect to ethical issues and fundamental rights.

In light of the above, the proposal has provided a series of reforms in the Europol Regulation as regards the agency's task to assist the Commission and Member States in identifying, developing and using new technologies for law enforcement purposes. In particular, the rules of Article 4 are expanded so that the agency can 'proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States, and implement its research and innovation activities […], including the development, training, testing and validation of algorithms for the development of tools'.[13] Emphasis is on the new technological solutions based on AI, whereby the agency shall play a key role in promoting 'ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety and fundamental rights'.[14] Furthermore, Europol will assist the Commission in identifying key research themes and drawing up and implementing the EU framework programmes for research and innovation activities that are relevant to achieve its objectives.

According to the proposal, Europol will not merely provide support to the EU security research programme, the Innovation Lab and Europol's support to the innovation hub,[15] but will be involved in research activities. In

[5] Valsamis Mitsilegas and Niovi Vavoula, 'Databases' in Valsamis Mitsilegas, *EU Criminal Law* (2nd edn, Hart 2022); Valsamis Mitsilegas and Fabio Giuffrida, 'Agencies, Bodies and Offices' in Valsamis Mitsilegas, *EU Criminal Law* (2nd edn, Hart 2022).

[6] Europol's engagement in the so-called 'hotspots' to carry out secondary security checks on TCNs arriving in the EU fostered the Agency's involvement in the processing of personal data within that area. The establishment of the European Migrant Smuggling Centre (EMSC) was a further step in deepening the sharing of intelligence between Europol and other authorities involved in border control and migration management. See David

[7] Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final. For an analysis see Niovi Vavoula and Valsamis Mitsilegas,

[8] Commission, 'Europol Impact Assessment Part 1' 30.

[9] https://data.consilium.europa.eu/doc/document/PE-8-2022-INIT/en/pdf

[10] Council, Document 12837/19 (7-8 October 2019).

[11] European Parliament 'Resolution of 18 December 2018 on findings and recommendations of the Special Committee on Terrorism' (P8_TA(2018)0512).

[12] Europol, 'Written contribution to JPSG The Europol Innovation Lab - May 2020', which may be found here <https://www.europarl.europa.eu/cmsdata/208046/Europol%20Contribution%20for%20Electronic%20exchange%20-%20Europol%20Innovation%20Lab.pdf> accessed 31 May 2022.

[13] Commission, 'Europol proposal' (n 6) art 1(2)(a)(iv). See recital 37.

[14] ibid recital 38.

[15] This is the case with the EBCG/Frontex. See Regulation (EU) 2019/1896 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 [2019] OJ L 295/1, art 66.

particular, the agency will also be enabled to process personal data for research and innovation matters for the development, training, testing and validation of algorithms for the development of tools.[16] This option has been preferred to address the need for an EU-level capacity to train, test and validate algorithms for the development of tools, including AI-based tools for law enforcement.[17] In addition, a new provision is inserted in that article prescribing that the processing of personal data for the purpose of research and innovation shall be performed by means of Europol's research and innovation projects with clearly defined objectives, duration and scope of the personal data processing involved, in respect of which additional safeguards will apply, as set out in the new Article 33a.[18] The latter lays down a series of rules on how personal data should be processed for research and innovation purposes, in particular:

1. Any project shall be subject to prior authorisation by the Executive Director, based on a description of the envisaged processing activity setting out:
    a. the necessity to process personal data, such as for exploring and testing innovative solutions and ensuring accuracy of the project results;
    b. a description of the personal data to be processed;
    c. a description of the retention period and conditions for access to the personal data;
    d. a data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome; and
    e. the measures envisaged to address those risks.
2. The Management Board and the EDPS shall be informed prior to the launch of the project.
3. Any personal data to be processed shall be temporarily copied to a separate, isolated and protected data processing environment within Europol for the sole purpose of carrying out that project, and only authorised staff of Europol shall have access to that data.
4. Any personal data processed shall not be transmitted, transferred or otherwise accessed by other parties.
5. Any processing of personal data shall not lead to measures or decisions affecting the data subjects.
6. Any personal data processed shall be deleted once the project is concluded or the personal data has reached the end of its retention period.
7. The logs of the processing of personal data shall be kept throughout the duration of the project and for an additional year, solely for the purpose of, and only as long as necessary for, verifying the accuracy of the outcome of the data processing.
8. Finally, the agency shall keep a complete and detailed description of the process and rationale behind the training, testing and validation of algorithms to ensure transparency and for the verification of the accuracy of the results.

Europol will acquire a pioneering role in shaping the future of law enforcement tools. From the outset, it must be clarified how the term 'innovation activities' is being defined and used. As the EDPS has stressed in his Opinion on the European Strategy of Data, the definitions and scope of key concepts related to research and innovation are not provided. [19] This approach may blur the boundaries between public interest, academic freedom and private gain and create uncertainty that may have an impact on the protection of fundamental rights. The revision of the

[16] Commission, 'Europol proposal of 2020' (n 6) art 1(5)(a)(ii). See new art 18(2)(e).
[17] Commission, 'Europol Impact Assessment Part 1' 55.
[18] Commission, 'Europol proposal' (n 6) art 1(5)(b). See new art 18(3a).
[19] EDPS, 'Opinion 3/2020 on the European Strategy of Data' (16 June 2020) para 40.

Europol Regulation is an opportunity to clarify the scope of such concepts and ensure consistency in the terminology used across legal instruments in data protection law.[20]

It is possible that when developing new technologies **extensive processing of large quantities of personal data** may be required, for example to create and test algorithms or for encryption, which are available to Europol. Expanding the processing activities of Europol constitutes a limitation of the rights to respect for private life (Article 7 of the Charter) and protection of personal data (Article 8 of the Charter). The potential impact of the processing of personal data in the development of algorithms to the principle of non-discrimination (Article 21 of the Charter) must also be taken into account. Therefore, it must be ensured that such processing is in line with the principles of necessity and proportionality, in accordance with Article 52(1) of the Charter. In that respect, it is recalled that in Opinion 1/15 on the EU/Canada PNR Agreement 'the systematic use of [PNR] data for the purpose of verifying the reliability and topicality of the pre-established models and criteria […] or of defining new models and criteria […] [must] not exceed the limits of what is strictly necessary'.[21] In a similar vein, the use of operational personal data, lawfully collected and stored by Europol to develop tools and provide solutions to facilitate the fight against serious crimes and terrorism, could be justified, if accompanied by efficient and appropriate safeguards.[22]

The addition of new Article 33a is a welcome development, as it includes concrete safeguards. These safeguards will constitute *lex specialis*, applicable to Europol as regards the processing of personal data for scientific purposes and, therefore, Article 13 and Chapter IX of Regulation (EU) 2018/1725, which impose strict limitations to the use of operational data, will not be applicable. That said, as the EDPS has noted, the proposed list of safeguards is the minimum and not exhaustive and, therefore, there is room for improvement, so as to bring the Europol Regulation as close to the prescriptions with Regulation (EU) 2018/1725 as possible. One key safeguard to be included is that the processing of personal data for research and innovation should take place **only if needed in order to reach the objectives of the project**.[23] Another important issue is, as the processing of personal data will involve the use of **real operational data**, **to enable the use of synthetic, anonymised or pseudo-anonymised personal data where possible**, which is mentioned in Article 13 of the Regulation (EU) 2018/1725. Whether the **processing of special categories of personal data, which are sensitive in nature, is also permitted for research and innovation purposes is also unclear** and the wording of Article 33a does not explicitly exclude the processing of special categories of personal data. However, the Impact Assessment accompanying the Europol proposal specifically excludes the processing of such data.[24] This approach is in line with Article 76 of Regulation (EU) 2018/1725, which permits the processing of 'only where strictly necessary for operational purposes'. Therefore, **it is necessary that the processing of special categories of personal data is explicitly excluded. If, however, Europol would be permitted to process special categories of personal data appropriate safeguards must be in place on the purpose for processing, the actors that would have access to that sensitive data and the accountability framework**.[25]

Furthermore, **other principles of data protection law not featuring in Article 33a should be taken into account, in particular the principles of data minimisation, data quality and privacy by design and by default**. Indeed, if low quality data are used in the development of algorithms for example, the higher the risk of non-discrimination. As it is mentioned in the Impact Assessment, 'whereas it may be challenging to assess the quality of all data used for building algorithms, it is essential to collect metadata and make quality assessment of the correctness and generalisability of the data'.[26] Moreover, and in line with the comments from the EDPS, **the scope of the research and innovation activities should be further refined by specifically and concretely linking the activities with the tasks of Europol** and clarifying their scope in a binding document, for instance adopted by the Management Board of Europol, which could be subsequently updated, if necessary.[27] That

[20] Also see Council, Document 5527/4/21 75.
[21] Opinion 1/15 ECLI:EU:C:2017:592, para 174.
[22] EDPS, 'Opinion 4/2021' ft 22.
[23] Council, Document 5527/4/21 51.
[24] Commission, 'Europol Impact Assessment Part 1' 75.
[25] EDPS, 'Opinion 3/2020' (n 258) para 40.
[26] Commission, 'Europol Impact Assessment Part 1' 76.
[27] EDPS, 'Opinion 4/2021' para 33.

binding document should be available to the EDPS prior to the launch of each project for information and consultation and the EDPS should be informed every time the document is updated, as appropriate. Finally, **the one-year retention period of the logs may not be sufficient for data protection purposes and therefore logs could also be kept for an additional period**, **so as to enable the EDPS to conduct supervision and audits**,[28] unless the EDPS would be required to conduct their supervision within a year from the completion of a project.

Another issue that merits further exploration is the extent to which the Commission proposal links to the EU Internal Security Strategy 2020-2025, which envisaged 'the creation of a European Innovation hub for internal security that would seek to deliver common solutions to shared security challenges and opportunities, which Member States might not be able to exploit alone'.[29] This hub would also work with the EBCGA/Frontex, CEPOL, the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA) and the Joint Research Centre. However, nowhere in the proposal is there a reference to the hub and it thus appears that Europol will get the lion's share, if not the monopoly, in supporting the Member States in developing technological tools for law enforcement. Furthermore, as Europol will support the Commission in identifying research themes, the agency is essentially envisaged to become the primary agenda-setter in research and innovation, though it operates within a framework of other agencies in the internal security domain.[30] Furthermore, this relationship between the Commission and Europol may become problematic and undermine the independence of the agency.[31] Similarly, the relationship between Member States' efforts in similar research and innovation must be further defined so that efforts are coordinated, synergies are created[32] and duplication is avoided.[33] In such case, additional safeguards as regards access to the personal data processed by Member States are also necessary and have been added during negotiations by the Council.[34] Consequently, the Council has further emphasised on the need for cooperation with relevant networks of Member States' practitioners and other agencies to drive innovation and foster synergies, within their respective mandates.[35] This is in line with the European Parliament Resolution, as mentioned earlier, which did not provide Europol with an exclusive role in promoting research and innovation.

III. European Border and Coast Guard: Extensive Agenda-Setting

Europol's efforts to increase its mandate have gone hand in hand with Frontex's increasing role in border management. The first major increase in this context has been the powers that the agency have acquired in the context of ETIAS[36] and VIS,[37] where the agency is responsible for defining, establishing, assessing *ex ante*, implementing, evaluating *ex post*, revising and deleting the screening rules that will be used for assessing the risk posed by applicants for ETIAS authorisations or residence permits and visa applicants. The agency has already set up an ETIAS Central Unit in this respect. Furthermore, representatives of the egancy will participate in the ETIAS and VIS Sceening Board and the ETIAS and VIS Fundamental Rights Boards. At the same time, the agency has been entrusted with taks relating to the correction and deleting incorrect data along with the relevant authorities at the national level.[38] This has led to concerns by the agency that with the operationalisation of

[28] Council, Document 5527/4/21 71.
[29] Commission, 'Communication on the EU Security Union Strategy'.
[30] Council, Document 5527/4/21 86-88, 95.
[31] ibid 92.
[32] For example with the European Network of Law Enforcement Technology Services (ENLETS).
[33] Council, Document 5527/4/21 57.
[34] ibid 71, where Member States ask for access. Also see Council, Document 5388/2/21 42.
[35] Council, Document 5388/2/21 recital 37.
[36] 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
PE/21/2018/REV/1
OJ L 236, 19.9.2018, p. 1
[37] 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
OJ L 248, 13.7.2021, p. 11
[38] ETIAS Regulation, art 55.

ETIAS, it will be flooded with such requests, thus the joint responsibility of correction and deletion of data is viewed rather negatively. This shows that the agency is only prepared to grow its powers, without consequent increase of its responsibilities.

Beyond the operation of information systems for third-country nationals, the EBCG also heavily lobbies in favour of further use of AI-based systems in the context of border management. This is in line with its mandate Frontex' mandate to support research and innovation and contribute to the development of the EU's Integrated Border Management. Frontex's intent has been to find synergies with ongoing AI studies and initiatives in the EU and contribute to a Europe-wide AI landscape by adding the border security dimension. Its 2020 report,[39] analysed nine case studies: automated border control, maritime domain awareness, machine learning optimisation, surveillance towers, heterogeneous robotic systems, small autonomous UAS, predictive asset maintenance, object recognition to detect suspicious vehicles or cargo and the use of geospatial data analytics for operational awareness and threat detection. The agency has clearly indicated its interest in reconsidering its rolein shaping the future landscape of AI-based capabilities in European border security. Previous research identified a number of potential roles in this context:[40] ranging from mapping of future requirements and opportunities associated with AI and AI-based systems in border security – an exercise with which Frontex already engages -, strengthening the knowledge and evidence base, such as conducting impact assessments (arguably the existing report barely touches upon the relevant challenges), facilitating information and knowledge exchange, gathering and sharing lessons learned or developing training and education materials/programmes for end users within Member States. As such, Frontex could take a role in developing or facilitating public awareness campaigns or educating policy. The agency could even facilitate coordination between different stakeholder groups (agencies, institutions etc), but on this the competition with Europol may become an issue, or support the development of national capabilities or multi-national/EU projects through sponsoring or hosting technology demonstrators. As a result, it is highly likely that Europol has requested an increased role in the emerging AI-based border management, the EBCG will soon follow.

IV. EUAA: Developing AI Tools beyond Its Powers and without Safeguards

Another agency of interest for this contribution is the EU Agency for Asylum (EUAA), former European Asylum Support Office (EASO), which fosters cooperation among EU Member States on asylum. As Tsourdi points out, since the past few years EUAA has seen an expansion of the scope of its activities, including its potential to influence national refugee status determination.[41] For the purposes of this research, the focus on the work of EUAA is elsewhere: the agency developed an AI-based Early Warning and Forecasting System to monitor the situation in third countries and to forecast the number of asylum applications that EU Member States may expect. In its 2020 report, the agency asserted using 'machine learning to analyse big data on conflict and disruptive events in countries of origin and transit in order to clarify the root causes of individuals displacement events'.[42] The rationale behind the development of this tool is to understand and predict arrivals of third-country nationals that might exert particular pressure on national asylum and reception authorities. This approach is based on the apparent payoffs of increased efficiency, improved preparedness and enhanced border security, also providing novel insights into the field of migration and asylum research. To do so, EUAA builds upon three types of data collected on past events, namely data from traditional countries of origin and transit (including social media monitoring), data on pressures at the EU's external borders, and data on the outcomes of previous asylum applications in the EU. The agency's algorithm predicts pressures up to four weeks in advance and suggests possible future medium-term scenarios using historical and current data. With regard to social media monitoring,

[39] Frontex, ARTIFICIAL INTELLIGENCE -BASED CAPABILITIES FOR THE EUROPEAN BORDER AND COAST GUARD FINAL REPORT' https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf

[40] Cox, Kate, Sarah Grand-Clement, Jacopo Bellasio & Giacomo Persi Paoli. 2017. 'From Lab to Field: Challenges and Opportunities for Operationalising Border Security Research'. Santa Monica, Calif: RAND Corporation. Non-public report.

[41] Evangelia (Lilian) Tsourdi, Holding the European Asylum Support Office Accountable for its role in Asylum Decision-Making: Mission Impossible? German Law Journal

[42] EASO, EASO Asylum Report, 2020, p. 57.

until 2019, EASO produced social media monitoring reports based on analysing posts of Facebook, Instagram, YouTube, and Twitter users that were related to EU asylum and migration issues (within the Arabic, Pashto, Dari, Urdu, Turkish, Russian, Tigrinya, Kurmanji Kurdish, Pidgin English, Hausa, Edo, as well as French communities).[43] In 2019, the EDPS issued a temporary ban on the production of social media monitoring reports due to issues of legality – essentially this was beyond the agency's mandate - and data protection concerns.[44] 'Social media users monitoring is a personal data processing activity that puts individuals' rights and freedoms at significant risk. It involves uses of personal data that go against or beyond individuals' reasonable expectations. Such uses often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate'. The EDPS underscored the important principles of 'purpose limitation' and 'data minimisation', whereby personal data should be collected only for 'specified, explicit and legitimate purposes. The EDPS' warning also dovetails with the aims of this comment because as the public discusses the data mining and surveillance techniques to predict, manage and stop migratory movements, such legal and social pressure over official institutions and corporations will likely increase.

In other words, EUAA is heavily invested in what is called 'predicitve analytics'. Interestingly, the development of such tools for predictive analytics is completely outside the scope of the Commission proposal for an AI Act. Civil society organisations have called for adding predictive analytics within the scope of the AI Act as a high-risk system or even banned on certain occasions.

V. eu-LISA: Designing the Future Direction of Information Systems for Third-Country Nationals

Based in Tallinn, eu-LISA was established to be entrusted with the tasks of developing and operationally managing the existing and forthcoming large-scale IT systems for third-country nationals. It is considered as one of the smallest decentralised agencies,[45] even though following the reform of its initial legal basis- Regulation (EU) No 1077/2011 -[46] the agency's mandate was significant reinforced by Regulation (EU) 2018/1726,[47] including due to the proliferation of information systems and the need to develop the interoperability components.

eu-LISA's work in the field of AI is directly intertwined with the inclusion of AI systems in the currently operational information systems (Schengen Information System, Visa Information System and Eurodac) and those currently under development, namely European Travel Information and Authorisation System (ETIAS) Entry/Exit System (EES) and . As noted elsewhere,[48] different AI-based tools are already foreseen in the legal bases of information systems; for example, ETIAS and VIS envisage the use of algorithmic profiling to sort out applications for travel authorisations, visas and residence permits. Besides, with the exception of ETIAS all information systems encompass biometric identification through both fingerprint and facial recognition. With regard to interoperability, AI may be deployed for the purposes of the Central Repository for Reporting and Statistics (CRRS), part of the interoperability architecture, for example to create a multilingual natural language interface, to support data quality assurance and advanced data analytics. Furthermore, eu-LISA is working with Frontex, within which the ETIAS Central Unit will be developed, on the integration of an AI-based screening system within the scope of ETIAS, which will allow for automated profiling of travellers on the basis of pre-defined risk indicators and screening rules.[49]

43

44

45 eu- LISA, 'Consolidated Annual Activity Report 2020' (2021) 55.

46 Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
OJ L 286, 1.11.2011, p. 1

47 Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011
PE/29/2018/REV/1
OJ L 295, 21.11.2018, p. 99

48 Niovi Vavoula, Artificial Intelligence at the EU Borders

49 https://www.eulisa.europa.eu/Newsroom/News/Pages/Call-for-Expression-of-Interest---eu-LISA-Industry-Roundtable-November-2021.aspx Furthermore,

Beyond its operational tasks in developing and testing technical solutions to implement existing policies, eu-LISA's work is also future-oriented. In 2020, eu-LISA published a research and technology monitoring report on potential uses of AI in the operational management of large-scale IT systems.[50] This research is based on Article 14(1) of Regulation (EU) 2018/1726 according to which the agency is entrusted with tasks relating to monitor developments in research relevant for the operational management of SIS II, the VIS, Eurodac, the EES, ETIAS, DubliNet and other large-scale IT systems. As a result, the agency is also empowered with specific research-related tasks, which can impact the future direction of the information systems. Indeed, eu-LISA has proposed the use of a number

Therefore, eu-LISA's work has a very distinct impact. This is notwithstanding the fact the agency does not have a clear fundamental rights mandate – according to Article 2(f) eu-LISA must ensure a high level of data protection – only 10% of its staff has a legal background and compared to other agencies eu-LISA does not have strong oversight mechanisms both internally (for example through a Fundamental Rights Officer) or externally. Arguably, this is because eu-LISA does not touch the content of the databases. However, the increasing role of eu-LISA in the management of information systems, for example, ensuring data quality is a strong argument in favour of aligning the standards of that agency with the prescriptions of other agencies.

VI. Interagency co-operation: Promotion of AI-based Tools

The promotion of AI-based tools is also evident through fora whereby different agencies participate and cooperate. In addition to the establishment of the Innovation Hub within Europol, in the Future Group on Travel Intelligence and Border Management, that was set up by Europol and Frontex in 2019, the two agencies submitted a joint report calling for a 'border and travel continuum' whereby 'border management […] [will] rely on automated targeting or screening systems for performing risk management on the travellers with advance information' combining data from different sources which would most likely require the use of AI to combine sources effectively.[51] Furthermore, the proposed next step is for the EU Innovation Hub for Internal Security, operated by Europol, to oversee a study: 'Frontex, Europol and eu-LISA could jointly sponsor an ESTS feasibility study under the framework of the EU Innovation Hub for this purpose. National, international and EU experts also from Commission, FRA and EDPS should be involved in conducting this study'.

VII. Conclusion

This article aimed to analyse the role of each agency on is own and their cooperation in terms of using and designing AI-based tools for border management. This holistic approach has enabled the reader to understand how each agency is significantly expanding its mandate in this context and is growingly setting out the agenda for future policy making in digitalisation. It is evident that each agency has become greedier in terms of getting access to personal data, without necessarily being accompanied by fundamental rights safeguards or monitoring/accountability mechanisms. For example, the article has noted how eu-LISA's work is still viewed as technical in nature, therefore oversight mechanisms and fundamental rights safeguards are hugely missing. Europol's mandate also needed further compliance with fundamental rights safeguards.

[50] eu-LISA https://www.eulisa.europa.eu/Publications/Reports/AI%20in%20the%20OM%20of%20Large-scale%20IT%20Systems.pdf

[51] Council, Document 6767/22. https://www.statewatch.org/media/3307/eu-council-europol-frontex-travel-intelligence-future-group-6767-22.pdf