ARTICLES

SCHENGEN AND EUROPEAN BORDERS
*edited by* Iris Goldner Lang

# ALGORITHMIC ACCOUNTABILITY THROUGH THE "HUMAN OVER THE LOOP" IN INTEROPERABLE AND EU AI-RELIANT LARGE-SCALE IT SYSTEMS FOR MIGRATION AND SECURITY

NIOVI VAVOULA*



ABSTRACT: Interoperability of large-scale IT systems and the deployment of Artificial Intelligence (AI) systems in the field of migration, asylum and border management have been two parallel developments at EU level. Legal scholarship has not yet addressed in detail the potential interplay of these two initiatives and this *Article* stressed that various interoperability components are either pre-requisites or enablers for the deployment of AI in the EU IT systems. The *Article* analyses how these AI-powered components are dealt with by the AI Act and highlights potential challenges in classifying them as high-risk AI systems. In this highly complex and opaque legal framework, the *Article* argues that algorithmic accountability through supervision, framed as the "human over the loop", is particularly important. Such supervision so far has focused on data protection-related matters, but the deployment of AI has implications beyond the contours of data protection law. The *Article* provides recommendations on how supervision of interoperable and AI-reliant IT systems should be reconceived to achieve algorithmic accountability. In this respect, the analysis focused not only on the role of national data protection authorities, but also on other actors with supervisory underpinnings.

KEYWORDS: algorithmic accountability – interoperability – large-scale IT systems – artificial intelligence (AI) – supervision – migration.

* Associate Professor of Cyber Policy, University of Luxembourg, niovi.vavoula@uni.lu.

EUROPEAN PAPERS
VOL. 9, 2024, NO 3, PP. 1228-1249
www.europeanpapers.eu
ISSN 2499-8249
doi: 10.15166/2499-8249/807

## I. Introduction

Much ink has been spilt on the legal challenges posed by the operationalisation of interoperability of EU large-scale IT systems (databases) for third-country nationals.[1] These systems are: the operational Schengen Information System (SIS), Visa Information System (VIS) and Eurodac and the forthcoming Entry/Exit System (EES), European Travel Information and Authorisation System (ETIAS) and European Criminal Record Information System for third-country nationals (ECRIS-TCN). At the same time, an increasing volume of literature focuses on how Artificial Intelligence (AI) could be harvested to promote neutrality, objectivity and standardisation in decision-making in the field of migration, asylum and border management and analyses the challenges of the deployment of AI on non-discrimination, data protection and effective remedies.[2] However, the interplay between interoperability and AI, that is the extent to which the former will enable the latter in being deployed in databases and whether certain interoperability components will be AI-powered as such, has so far been relatively off the academic radar.[3]

This *Article* has a threefold aim; first, it fills this literature gap by shedding light into whether the operationalisation of interoperability will rely on AI systems arguing that most interoperability components are AI-enablers or AI-powered. Whereas it is often argued that algorithms pose a so-called "black box problem", whereby the algorithms might not be transparent enough, in the case of interoperability the challenges are even more acute, because the use of AI is unclear. Second, the *Article* classifies these AI systems in accordance with Regulation (EU) 2024/1689 (hereinafter AI Act) and demonstrates the underlying difficulties and challenges in such classification.[4] In light of this complex ecosystem whereby the use of AI is not straightforward, the *Article*'s third aim is to provide insights into the role of supervision as a mechanism for increasing algorithmic accountability. The latter has been elaborated in a multi-disciplinary literature.[5] Legal scholars focus on the improving

[1] E Brouwer, 'Large-scale databases and interoperability in migration and border policies: The non-discriminatory approach of data protection' (2020) EPL 71; T Quintel, 'Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention' (University of Luxembourg Working Paper 002-2018) 1; N Vavoula, 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?' (2020) EPL 131.

[2] D Ozkul, 'Automating immigration and asylum: The uses of new technologies in migration and asylum governance in Europe' (AFAR Report, 2023); N Vavoula, 'Artificial Intelligence (AI) at EU Borders: From Automated Processing to Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' (2021) European Journal of Migration Law 457.

[3] A Karaiskou and N Vavoula, 'Contesting the unknown: Algorithm-assisted decision-making and access to justice in the cases of ETIAS and VIS' (2025) German Law Journal (forthcoming).

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

[5] M Busuioc, 'Accountable artificial intelligence: Holding algorithms to account' (2020) Public Administration Review 825; J Kroll, J Huey, S Barocas, E Felten, J Reidenberg, D Robinson and H Yu, 'Accountable Algorithms (2017) UpaLRev 633.

the transparency of algorithmic systems, making them more understandable and explainable.[6] McGregor, Murray and NG suggest a more holistic approach, whereby the overall algorithmic life cycle is addressed, including monitoring and oversight mechanisms as safeguards and providing a remedy to individuals and groups whose rights have been allegedly violated.[7] This *Article* will specifically focus on algorithmic accountability through supervision of large-scale IT systems to highlight the opportunities and challenges of supervising interoperable and AI-reliant IT systems. Whereas emerging literature focuses on the "human in the loop" as a means of ensuring meaningful human control, whereby the human input and expertise is integrated into the lifecycle of AI systems,[8] this *Article* examines the "human over the loop" as a pivotal safeguard to improve algorithmic accountability.

The *Article* is structured as follows: the next section provides a synopsis of the EU legislative framework on interoperability, comprised of Regulations (EU) 2019/817 and 2019/818 (hereinafter Interoperability Regulations).[9] Section 3 examines how interoperability is intertwined with AI and the application of the AI Act in this context. Then, section 4 shifts the attention to the supervision of interoperable and AI-reliant IT systems calling for rethinking how the "human over the loop" could provide meaningful supervision of this complex architecture. The last section summarises the findings of the research.

## II. Interoperability of large-scale IT systems for third-country nationals: a synopsis

### II.1. The road

SIS, VIS and Eurodac were developed following a compartmentalised approach; the data jars remained physically separate from each other, due to the distinct institutional, legal, and policy frameworks within which they were developed. Debates on interconnecting databases fueled with the Commission Communication on improved effectiveness, enhanced interoperability, and synergies among EU databases, where interoperability was defined as the "ability of IT systems and of the business processes they support to exchange data and

[6] S Wachter, B Mittelstadt and C Russell, 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR' (2018) Harvard Journal of Law & Technology 841.

[7] L McGregor, D Murray and V Ng, 'International human rights law as a framework for algorithmic accountability' (2019) ICLQ 309.

[8] U Agudo, Liberal K, Arrese M and Matute H, 'The impact of AI errors in a human-in-the-loop process' (2024) Cognitive Research: Principles and Implications 1; S Alon-Barkat S and M Busuioc, 'Human–AI interactions in public sector decision making: From "automation bias" and "selective adherence" to algorithmic advice' (2023) Journal of Public Administration Research and Theory 153.

[9] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019.

to enable the sharing of information and knowledge".[10] However, specifications on the legal elements of interoperability were spared, as the concept was deemed solely as a technical rather than a legal or political issue.[11] In 2015, interoperability gained fresh impetus; the Communication on stronger and smarter information systems for borders and security criticised the "fragmentation" in the architecture of databases which are "rarely inter-connected".[12] The Interoperability Regulations were adopted in May 2019 and at the time of writing, the preparations for setting up interoperability in the IT systems alongside developing EES, ETIAS and ECRIS-TCN are underway, targeting 2027 for full implementation.[13]

### II.2. The Interoperability Regulations

Interoperability is the ability "to exchange data and to share information so that authorities and competent officials have the information they need, when and where they need it".[14] It will enable additional data processing operations via aggregating specific personal data from the different data pots. Interoperability was intended to have various positive results: enabling seamless, faster and more systematic access to information, as well as the detection of individuals who use multiple identities, facilitating identity checks of third-country nationals, and streamlining law enforcement access.[15] Interoperability involves the combination of existing data in new ways and pooling *certain* data to give way to simplified processes, such as identification of individuals on national territory. It involves the establishment of five interoperability components: the European Search Portal (ESP), the shared Biometric Matching Service (sBMS), the Common Identity Repository (CIR), the Multiple Identity Detector (MID), and the Common Repository for Reporting and Statistics (CRRS), each of which are outlined below.

[10] Communication COM(2005) 597 final from the Commission of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs 3.

[11] P De Hert and S Gutwirth, 'Interoperability of police databases within the EU: An accountable political choice?' (2006) International Review of Law Computers & Technology 21, 22.

[12] Communication COM(2016) 205 final from the Commission of 6 April 2006 on stronger and smarter information systems for borders and security 3-4.

[13] Statewatch, *Database delays: new timetable for interoperable EU policing and migration systems by 2027* www.statewatch.org.

[14] Proposal COM(2017) 793 final from the Commission of 12 December 2017 for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226; Proposal COM(2017) 794 final from the Commission of 12 December 2017 for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 1.

[15] Proposal COM(2017) 793 final cit.; Proposal COM(2017) 794 final cit. 15.

*a) ESP: single query, combined results*

According to art. 6 of the Interoperability Regulations, ESP will serve as a single window or "message broker" enabling national and EU authorities to query at the same time the underlying systems, Europol data and the Interpol databases to which they have access, without the need to conduct searches to each database separately. The individual results will be displayed on a single screen. ESP will also be used for automatically querying all databases in the course of examining applications for travel authorisations (ETIAS), visas and residence permits (VIS). In addition, Prüm data – namely, DNA profiles, dactyloscopic data and vehicle registration data, facial images and police records exchanged in the framework of police cooperation – can be searched through ESP in line with Regulation (EU) 2024/982.[16] The same applies to Advanced Passenger Information (API), though at the time of writing the relevant rules have been agreed but not officially published.

*b) sBMS: a database for biometric templates*

sBMS will be a new database storing biometric *templates* of the biometric data recorded in all IT systems, except ETIAS, which does not envisage the processing of such data. According to art. 4(12) of the Interoperability Regulations, a template is a "mathematical representation obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications". The template only represents particular features selected by the algorithm(s) and does not contain all the biometric information of the sample collected.[17] sBMS will regroup the templates to enable searches of biometric data through a shared, common platform for cross-checking them at the same time, whilst retaining the templates logically separated depending on the system. Its purpose is to facilitate identifying persons whose personal data are recorded in several databases through a single tool that will match their biometric data across different databases.

*c) MID: A Novel Tool*

MID will create, retain and label links between identical data indicating whether individuals are registered in more than one system for a legitimate reason, or whether there is a potential case of identity fraud. Its double purpose is on the one hand, to facilitate identity checks for *bona fide* travellers, and on the other hand to combat identity fraud. Multiple identity detection will take place at various *loci*; at the border, or on national territory in a random check. It will also operate continuously whenever data on a particular individual are processed within any database. The Interoperability Regulations envisage four types of links, with colour coded suspicion levels. When the multiple detection process is complete, all links will be either white or yellow. A white link will indicate that the data involve the same person (clear identity). Yellow links will denote situations of unclear identity, whereby the identity data are not similar, but a case of different identities has not yet been confirmed.

[16] Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024.

[17] E Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer 2013) 98.

Following manual verification, yellow links will become green, white or red. Green links will mean that the linked data correspond to different persons (e.g. twins). In turn, a red link will indicate identity fraud, either through use of different identities in an unjustified manner or by another person's identity.[18]

*d) CRRS: The Non-personal Data Database of Statistical Data*

The last interoperability component is CRRS, envisaged in art. 39 of the Interoperability Regulations. It will support the objectives of the IT systems, all of which foresee the compilation of statistical data.[19] These serve as metrics of their performance to assist in evidenced policy making, evaluation of their functioning and possible legislative revisions. At the same time, CRRS will provide "cross-system statistical data and analytical reporting for policy, operational and data quality purposes".[20] According to Delegated Regulation (EU) 2021/2223,[21] the cross-system statistical data will come from the underlying EU information systems, sBMS, CIR and MID. CRRS must hold only anonymous data, not allow for the identification of individuals and operates on the basis of Commission Delegated Regulations 2021/2223 and 2021/1224, which envisage the development of both "statistical reports" defined as an organised collection of statistical data, produced in an automated manner according to a set of pre-established rules,[22] and "'customisable reports' [that] means statistical reports [...] extracted on the basis of statistical data contained in the central repository in accordance with specific rules".[23]

## III. Searching for AI in Terminologically Ambiguous Texts

No legal instrument governing the IT system or interoperability and no implementing or delegated act mentions the term "AI". However, art. 111 of the AI Act states that "AI systems which are components of the large-scale IT systems [...] that have been placed on the market or put into service before 2 August 2027 shall be brought into compliance with this Regulation by 31 December 2030". The legal instruments governing the databases and their interoperability are listed therein. This delay in bringing the large-scale IT systems within the scope of the AI, coupled with art. 83 of the Commission Proposal for

[18] Art. 32 Interoperability Regulations cit.

[19] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017, art. 63; Regulation (EU) 767/2008 of the European Parliament and Council of 9 July 2008, art. 17; Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018, art. 84; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018, art. 60; Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018, art. 16.

[20] Art. 39(1) Interoperability Regulations cit.

[21] Commission Delegated Regulation (EU) 2021/2223 of 30 June 2021.

[22] Art. 1(2) Delegated Regulation 2021/2223 cit.

[23] Art. 1(3) Delegated Regulation 2021/2223 cit.

an AI Act which *ab initio* excluded them from the scope,[24] is peculiar and points to the direction that the IT systems will rely on AI tools, so this section will examine precisely whether and to what extent this is the case.

### III.1. The pivotal role of the CRRS

Reference to "algorithms" is made in Regulation 2018/1240 on ETIAS and the Regulation 2021/1134 on VIS to refer to the automated processing of applicants for travel authorisations (for visa-free nationals) and Schengen visas against various European and international databases, as well as what are called "screening rules" (in ETIAS) or "specific risk indicators" (in VIS).[25] These algorithms enable the profiling of travellers to determine whether they pose a risk to irregular migration, security or public health. They will be developed by the ETIAS Central Unit, established within the European Border and Coast Guard Agency (EBCG Agency). The risk indicators based on which the algorithms must be developed must be defined through various statistical data including data provided by the IT systems themselves. Recourse to the term "algorithm" may be seen as either a means of avoiding the loaded term of "AI" or as leaving this issue open for introducing AI in the future. Even the term algorithm has been contested; Frontex has insisted that it would actually be more appropriate to refer to filtering queries than algorithms, and that no sophisticated analysis methods or any form of AI is involved in the risk assessment.[26] As Zandstra and Brouwer stress, this approach is at odds with the very wording of the legal instruments and exemplifies the politics around the use of AI this field aimed at blurring the landscape and ultimately obstruct scrutiny.[27]

The potential of using AI in the implementation of the ETIAS screening rules and the VIS specific risk indicators may be found in CRRS, aimed to provide cross-system statistical data and analytical reporting for policy, operational and data quality purposes.[28] A (non-publicly available) report by eu-LISA states that CRRS, that will collect and store (among others) statistical data from VIS, EES and ETIAS of over-stayers and information regarding refusals of entry of third-country nationals, can use AI tools to enhance the identification of risks for specific groups of travellers by identifying patterns or a set of

[24] Proposal COM(2021) 206 final from the Commission of 21 April 2021 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 act.

[25] art. 33(1) Regulation 2018/1240 cit. and art. 9(j)(1) Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021.

[26] C Derave, N Genicot and N Hetmanska, 'The risks of trustworthy artificial intelligence: The case of the European Travel Information and Authorisation System' (2022) European Journal of Risk Regulation 389

[27] T Zandstra and E Brouwer, 'Fundamental rights at the digital border: ETIAS, the right to data protection, and the CJEU's PNR judgment' (24 June 2022) Verfassungblog verfassungsblog.de.

[28] A Karaiskou, 'Immigration and Algorithmic Discrimination in Europe' (Ph.D. Thesis, European University Institute).

common characteristics from the analysis of historical data in the CRRS related to security, irregular migration and high epidemic risks.[29] Furthermore, in its Report of the Future Group on Travel Intelligence and Border Management by Europol and the EBCG Agency, it is stated that in cooperation with eu-LISA and other partner agencies, the joint analysis capability could leverage the full potential of CRRS as a data source for analytical purposes and develop appropriate analytical tools for risk assessment with the support of AI.[30] The possibility that CRRS could use AI tools to assist in the design of risk profiles for ETIAS and VIS demonstrates the true potential of the interoperability components, which is not exhausted in aggregating data from the underlying systems, but entails putting them into novel uses beyond the contours of their operation.

The use of AI in CRRS for the determination and verification of the risk profiles raises the question of how to classify it in light of the AI Act. In light of Annex, it seems appropriate that CRRS could be categorised as "AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State".[31] This is a high risk AI system which requires safeguards on risk management,[32] human oversight,[33] pre-market conformity assessments,[34] and post-market monitoring.[35] Furthermore, both providers and deployers also need to register specific information of the high-risk AI systems in a EU database managed by the Commission in collaboration with the Member State concerned.[36] However, high-risk AI systems in the area of migration, asylum and border control management will be registered in a *non-public* database only accessible to the Commission and competent national authorities.[37] Furthermore, certain important pieces of information, such as the training data used or a summary of the fundamental rights impact assessment, do not need to be entered at all.[38] This is a particularly important exception because it may perpetuate the lack of transparency regarding the use of AI in ETIAS and VIS. As a result, we may never have full information regarding the application of AI in CRRS.

In addition, according to art. 6(3) any high-risk AI system shall not be considered to be high risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome

[29] Eu-LISA, 'AI in CSSR in the context of ETIAS and the revised VIS' (Report 2022).

[30] Europol and EBCG Agency, 'Future group on travel intelligence and border management' (Report 2021) 65.

[31] Para. 7(b) Annex III Regulation 1689/2024 cit.

[32] Art. 9 Regulation 1689/2024 cit.

[33] Art. 14 Regulation 1689/2024 cit.

[34] Art. 17 Regulation 1689/2024 cit.

[35] Art. 72 Regulation 1689/2024 cit.

[36] Art. 49 in conjunction with art. 72 Regulation 1689/2024 cit.

[37] Art. 49(4) Regulation 1689/2024 cit.

[38] Art. 49(4) in conjunction with Annex VIII Regulation 1689/2024 cit.

of decision making. The conditions for applying this derogation are: (a) the AI system is intended to perform a narrow procedural task; (b) the AI system is intended to improve the result of a previously completed human activity; (c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or (d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III. In this case, it is likely that conditions (c) or (d) could apply resulting in decategorising CRRS to a limited risk AI system, thus removing the protective standards of the AI Act. However, art. 6(3) contains an exception for AI systems performing profiling of natural persons, which means that as the CRRS will assist the algorithmic profiling in ETIAS and VIS, it should always be considered as high-risk AI system.

Whereas at present the potential of using AI in ETIAS and VIS risk assessment is hidden into the different technical specifications of the systems, the future orientation of these assessments is a bit clearer. AI tools could enhance the automated processing of textual information by detecting common textual characteristics in manually uploaded data and will facilitate the identification of specific groups of risky travellers. According to eu-LISA, ETIAS can employ AI tools in different ways: first, to review and validate the *ex-ante* assessment process of screening rules assisting officers in the examination of the application by using stored and historical data and generating an indicator for normal and suspicious outcomes for a specific set of travellers.[39] Second, AI could be embedded in ETIAS in the identification and analysis of correlations amongst the risk profiles from its own historic data to allow more precision in the definition of the risk profiles. Third, AI tools could analyse, detect deviations and propose further review of the risk indicators during the ex-post assessment process. Finally, AI technology could support the verification of hit, using ETIAS historical data by implementing model training of the corresponding risk profiles. The extent to which this is embedded remains unclear, but the mere existence of the eu-LISA report indicates that all options are open. The report's suggestions are in line with the Commission's vision on the use of AI in the field of migration to identify irregular travelling patterns as an additional piece of risk analysis implement a second profiling tool following the first one.[40]

### III.2. sBMS: motor for biometric recognition

Biometric recognition operates based on the concept that humans can be recognised automatically by employing a system like human interaction. This umbrella term encompasses two functions: biometric verification or one-to-one (1:1) recognition and biometric

[39] Eu-LISA, 'Artificial intelligence in the operational management of large-scale IT systems' (Report 2020).

[40] Directorate-General for Migration and Home Affairs of the European Commission and Deloitte, 'Opportunities and challenges for the use of Artificial Intelligence in border control, migration and security' (Report 2020).

identification, known as one-to-many recognition (1:N). With the exception of ETIAS, IT systems will process different types of biometric data, with emphasis on verification and identification initially through fingerprints and more recently facial images.

Fingerprint identification already takes places in Eurodac, VIS and SIS to verify the identity or identify third-country nationals at the borders or on national territory.[41] There is also urge in making the most of facial images, through the deployment of facial recognition technology (FRT), which is more invasive as it happens at a distance, without contact, with people in motion, without their awareness or consent.[42] All EU large-scale systems, except ETIAS, will process facial images and fingerprints. For example, in SIS, facial images will not only be used to confirm the identity of a person, but also to identify a person in the context of regular border crossing points.[43] In delegated acts, the Commission will also determine "other circumstances in which photographs and facial images may be used to identify persons".[44] For instance, it is likely to use "computer vision to detect SIS alerts using cameras" deployed at border points.[45] The police checks envisaged in art. 20 of the Interoperability Regulations will take place through biometric data. sBMS, will become the motor for biometric verification and identification real-time or remote and CIR will play a key role in biometric matching, as it will store certain biographic and the biometric data of the systems.[46]

That FRT will rely on AI is confirmed by eu-LISA itself.[47] In the case of EES, eu-LISA further states that the system will rely on machine learning techniques for biometric matching.[48] In the case of SIS, the processing of facial images will take place by "plugging CCTV cameras into an AI-enabled, EU-wide police database so that wanted or suspected individuals can be tracked down via their faces or vehicle number plates".[49] AI in FRT can improve the accuracy of identification and verification.[50] This does not mean that AI in the fingerprint processing is off limits. Preetha and Sheela suggest that machine learning

[41] N Vavoula, 'Artificial Intelligence (AI) at EU Borders: From Automated Processing to Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' cit.

[42] *Ibid.*

[43] Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018, art. 33(4).

[44] art. 33(4) Regulation 2018/1861 cit.

[45] Directorate-General for Migration and Home Affairs of the European Commission and Deloitte, 'Opportunities and challenges for the use of Artificial Intelligence in border control, migration and security' cit. 63.

[46] Eu-LISA, 'Artificial intelligence in the operational management of large-scale IT systems' cit.

[47] Eu-LISA, *Schengen Conference Session 8 AI but also Interoperable and Automated + Conclusion of the Conference – Intervention by Luca Tagliaretti, Deputy Executive Director of Eu-LISA* www.youtube.com.

[48] Eu-LISA, 'Artificial intelligence in the operational management of large-scale IT systems' cit.

[49] EuroMed Rights, 'Europe's techno borders' (Report 2023) 21.

[50] N Menéndez González, 'The impact of facial recognition technology empowered by artificial intelligence on the right to privacy' in D Bielicki (ed) *Regulating artificial intelligence in industry* (Routledge 2022) 21-35.

(ML) techniques, such as Artificial Neural Networks (ANN), Deep Neural Networks (DNN), Support Vector Machine (SVM) and Genetic Algorithms (GA), may assist in cases of fingerprint identification problems, due to skin conditions, damaged fingerprint, scars or small fingerprint surface area.[51]

The potential of integrating AI brings to the fore the application of the AI Act, which regulates remote biometric identification as a high-risk AI system in a horizontal manner irrespective of their specific use. Furthermore, AI systems intended to be used for biometric verification of someone's identity are considered as posing a limited risk to fundamental rights. This is notwithstanding the fact that biometric verification poses significant challenges to non-discrimination due to lack of reliable algorithms in respect of black people and women (and irrespective of whether the biometric recognition involves verification or identification).[52] On the plus side, in the case of biometric identification a higher standard is set requiring that every action or decision based on the AI system must be reviewed by at least two competent persons.[53] This is justified with the "significant consequences" an incorrect match can have for people.[54]

### III.3. MID: an AI-powered interoperability component?

The operation of MID entailing the cross-checking of personal data against all records and the automated creation of links among datasets and the fingerprint matching in national Automated Fingerprint Identification Systems (AFIS) may also entail the use of AI. First, according to art. 27(2) of the Interoperability Regulations, where a record contains biometric data, the detection will be performed through sBMS, Thus, FRT will be used for comparing the biometric templates created from new data to the templates already stored to determine whether data of the same person are already stored in CIR or SIS. Second, with regard to alphanumeric data, searches in ESP will take place using different combinations of certain biographical data or travel document data.[55] In that regard, according to Recital 41 of the Interoperability Regulations, small transliteration or spelling mistakes will be detected in a manner to avoid creating any unjustified inconvenience for the person in question. Indeed, Commission Delegated Regulation 2023/333 stresses the need to ensure that the number of cases in which yellow links are generated by MID and therefore require manual verification are limited.[56] To that end, the Commission Delegated Regulation provides an exhaustive list of rules for when identity data shall be considered as similar. These rules

[51] Preetha S and Sheela S, 'Analysis of Fingerprint Biometric Authentication Using CNN' (2021) Social Science Research Network papers.ssrn.com.

[52] B Sumer, 'The AI Act's exclusion of biometric verification: Minimal risk by design and default?' (LAILEC Research Colloquium, Leuven, 7 June 2024).

[53] Art. 14(5) AI Act cit.

[54] Recital 73 AI Act cit.

[55] Art. 27(3)-(4) Interoperability Regulations cit.

[56] Commission Delegated Regulation (EU) 2023/333 of 11 July 2022.

concern, for example, known transliteration of names, inversions of name and surname, cases of the order of letters being inversed, or where a difference is found due to the use of hyphens, inversion of date and month when these match. The rules must be applied by eu-LISA, assisted and advised by the Interoperability Advisory Group, "by means of an algorithm in consultation with the Commission assisted and advised by the Interoperability Subgroup of the Expert Group on Information Systems for Borders and Security".[57] eu-LISA shall monitor the impact of the application of the algorithm and report, on a regular basis, to the Expert Group. Where necessary, to limit the number of cases in which yellow links generated by the multiple-identity detector would need to be turned into white links by the responsible authorities, the Commission, assisted and advised by the Expert Group, shall request eu-LISA to adjust the algorithm by prioritising the yellow links created between identity data that are considered more similar.

The algorithm based on which the MID will conduct the multiple identity detection based on alphanumeric data could rely on AI for text comparison and detection of similarities and difference.[58] However, the application of the AI Act is challenging. Among the high risk AI systems in the field of migration, asylum and border management listed in art. 7, Annex III. MID could fall under any of these two categories: MID could be considered as a risk assessment,[59] aimed at determining whether the individual commits identity fraud, thus broadly speaking whether they pose a risk of irregular migration or a security risk. This category relates to profiling whereby here the profiling performed by MID involves an analysis of "aspects concerning that natural person's [...] reliability or behaviour" in accordance with art. 4(4) of the Regulation 2016/679 (General Data Protection Regulation, hereinafter GDPR),[60] and art. 3(4) of the Directive 2016/680 (Law Enforcement Directive, hereinafter LED).[61] The second option is to consider MID a tool for "the purpose of detecting, recognising or identifying natural persons",[62] as MIS will enable the correct identification of bona fide persons and combating identity fraud.[63] Furthermore, combatting identity fraud relates to law enforcement. According to art. 5(1)(d), AI systems used to assess or predict the risk of a natural person committing a criminal offences, based solely on profiling or on assessing their personality traits and characteristics are prohibited. In turn, AI systems used in support of law enforcement authorities for the profiling of natural persons in the course of the detection, investigation or prosecution of criminal offences are high risk.

Given that yellow links require human action and assessment to be transformed into another colour-coded link, MID cannot be considered as a fully-fledged profiling tool, but

[57] Para. 2 Annex II Commission Delegated Regulation 2023/333 cit.

[58] F Tassinari, 'The external reach of the interoperability of large-scale IT systems in the AFSJ' (PhD Thesis, University of Granada, 2022) 429

[59] Para. 7(b) Annex III AI Act cit.

[60] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

[61] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016

[62] Para. 7(d) Annex III AI Act cit.

[63] Proposal COM(2017) 793 final cit. and Proposal COM(2017) 794 final cit. 7

as a tool that *supports* such assessment by flagging cases of potential identity fraud. However, at the same time MID is also a tool that assists in identification of third-country nationals, thus, MID constitutes a *hybrid* tool. This hybrid nature presents a major challenge. As mentioned above, art. 6(3) of the AI Act allows for declassifying a high-risk AI system under certain requirements, with the exception of AI systems performing profiling. In the case of MID it is likely that conditions (a) or (d) could apply; this means that if MID is classified as a profiling tool then it cannot be declassified, whereas if considered as an identification tool such decategorisation can take place.

## IV. Algorithmic accountability through the "human over the loop"

The previous section highlighted that the interplay between interoperability and AI is hidden behind terminological ambiguities in legislative and non-legislative EU instruments and technical and political games obstructing transparency and foreseeability. These developments, coupled with the ongoing revisions of the legal instruments, challenge the principle of transparency, enshrined in art. 5(1)(a) of the GDPR and more broadly the rule of law, preventing accessibility and foreseeability of the underlying rules. To open this "black box", enhancing algorithmic accountability through the "human over the loop", who will oversee the processing of personal data in the interoperability and AI-reliant architecture, emerges as a urgent necessity. There are three types of authorities, or constellations of authorities, which can play a role in monitoring the law and its implementation at national and EU level; (a) Data Protection Authorities (DPAs) and the European Data Protection Supervisor (EDPS), as the traditional supervisory authorities of the large-scale IT systems; (b) the Fundamental Rights Guidance Boards, set up in connection with ETIAS and VIS, with an advisory role on the use of algorithms for pre-vetting applicants for travel authorisations and visas and (c) the "market surveillance authorities", envisaged in the AI Act. This section outlines how supervision is organised and highlights the benefits and challenges of these structures.

### IV.1. DPAs and EDPS

Supervision is recognised as a constitutive element of the right to protection of personal data under art. 8(3) of the EU Charter of Fundamental Rights.[64] Supervision is entrusted to national DPAs, which operate in line with the GDPR or the LED in respect of personal data processing occurring at the national level (by public or private entities). Supervision of EU institutions, agencies and bodes is entrusted to the EDPS. DPAs constitute independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law and they provide expert advice on data protection-related issues and handle complaints lodged against violations of EU data protection law and relevant national laws. Their role has been highlighted by the Court of Justice of the European

[64] Charter of Fundamental Rights of the European Union [2012].

Union (CJEU) in various cases.[65] According to Tas,[66] supervisory authorities serve three distinct purposes; to ensure the observance of the law, to promotion of market integration, the internal market and competition and they are guardians of fundamental rights and freedoms.[67] Furthermore, supervision enables accountability;[68] as the EDPS has pointed out, they "provide support to the EU institutions to be accountable", and they "aim to develop a culture of accountability".[69] Can they supervise interoperable and AI-reliant IT systems, and if so, how?

*a) Supervision of large-scale IT systems*

Supervision is organised in a two-tiered approach; the EDPS supervise the central unit of such large-scale IT systems and the processing by EU agencies (Europol, EBCG Agency) to the extent that they have access to the systems. The use made of them by Member States' authorities is supervised by the national DPAs. The legal bases of the IT systems lay down specific rules on how supervision must take place, as follows: audits must be conducted under different timeframes: at least every four years in the cases of SIS, VIS and interoperability,[70] and at least every three years for EES, ETIAS and ECRIS-TCN.[71] In relation to Eurodac, the Member States are only required to do so in respect of law enforcement access to the data on a yearly basis and by an independent body.[72] In the case of SIS, the audit shall either be carried out by the supervisory authorities, or the supervisory authorities shall directly order the audit from an independent data protection auditor.[73] Furthermore, the DPAs must have sufficient resources to fulfil the tasks entrusted to them and have access to advice from persons with sufficient knowledge of biometric data (in the case of SIS and Eurodac) or in general expertise in the case of interoperability and

[65] Case C-518/07 *European Commission v Federal Republic of Germany* ECLI:EU:C:2010:125; Case C-320/03 *European Commission v Republic of Austria* ECLI:EU:C:2005:684; Case C-808/18 *European Commission v Hungary* ECLI:EU:C:2020:1029.

[66] S Tas, 'Overseeing supervision - Europol's processing and exchanges of personal data' (PhD Thesis, European University Institute, 2023) 58.

[67] O Lynskey O, 'The "Europeanisation" of data protection law. Cambridge Yearbook of European Legal Studies' (2017) CYELS 252, 283.

[68] S Tas, 'Overseeing supervision - Europol's processing and exchanges of personal data' cit. 68-70.

[69] EDPS, *Our Role as an Advisor* www.edps.europa.eu.

[70] Art. 55(2) Regulation 2018/1861 cit.; Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018, art. 69(2); Regulation (EU) 2008/767 of the European Parliament and of the Council of 9 July 2008, art. 41(2) and art. 51(3) Interoperability Regulations cit.

[71] Art. 55(2) Regulation 2017/2226 cit.; art. 66(4) Regulation 2018/1240 cit. and Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019, art. 28(2).

[72] Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024, art. 46(2).

[73] Art. 55(2) Regulation 2018/1861 cit. and art. 69(2) Regulation 2018/1862 cit.

ETIAS.[74] Specific rules exist regarding supervision of eu-LISA as the agency responsible for the operational management of the IT systems.[75]

At the heart of the supervisory arrangements is coordinated supervision, whereby the DPAs and the EDPS actively cooperate, by exchanging relevant information, assisting each other in conducting audits and inspections, examine difficulties in interpreting relevant rules, study problems that are revealed through supervision or the exercise of the data protection rights, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary. Twice per year the DPAs and the EDPS must meet as part of the European Data Protection Board (EDPB), which has set up a standing Committee for this purpose, the Coordinated Supervision Committee (CSC). Before the establishment of this Committee, Supervision Coordination Groups (SCGs) operated in respect of each operational systems (SIS, VIS and Eurodac). CSC, set up by art. 52 of Regulation 2018/1725, is a step further as it ensures harmonised supervision, which is vital in an interoperable environment, whereby the challenges ahead may be common across the systems and require common approach.

In the past years, supervision has focused on the exercise of individual rights, providing opinions on proposed legislation, participation in audits and the Schengen Evaluation teams among other tasks. However, DPAs' work has been significantly impacted by the lack of financial and human resources to effectively and independently carry out their envisaged supervisory tasks.[76] Supervision has been a complex task, also due to the constant need for the DPAs and the EDPS to adapt to the constant reforms to the underlying legal framework and the fact that the enforcement of the GDPR has got the lion's share for DPAs.

*b) The "human over the loop" must get their hands dirty*

Interoperable presents novel challenges for supervision. First, the legal instruments regulating the operation of large-scale IT systems are highly complex on their own and as part of the interoperability framework. They generally follow a similar structure, but there are particularities due to different objectives and functions, therefore familiarity with the legal framework is neither an easy nor a straightforward task. Furthermore, supervision concerns an increasing number of domestic users (border, visa, immigration, asylum, law enforcement authorities) as well as EU actors, such as Europol, eu-LISA and the EBCG Agency.

[74] Art. 55(3) Regulation 2018/1861 cit.; art. 69(3) Regulation 2018/1862 cit.; art. 41(3) Regulation 2008/767 cit.; art. 55(3) Regulation 2017/2226 cit.; art. 66(5) Regulation 2018/1240 and art. 51(4) Interoperability Regulations cit.

[75] Art. 70 Regulation 2018/1862 cit.; art. 42(2) Regulation 2021/1134 cit.; art. 42(2) Regulation 2024/1358 cit.; art. 56(2) Regulation 2017/2226 cit.; art. 66(2) Regulation 2018/1240 cit.; art. 29(2) Regulation 2019/816 cit. and art. 52(2) Interoperability Regulations cit.

[76] SIS II SCG, *Letter on the lack of financial and human resources given out to the data protection authorities* www.edps.europa.eu.

With interoperability the data flows will become even more complex, calling into question how the audits can take place. The reference to the phrase "at least" allows audits to take place before the four-year or three-year mark. In this regard, I argue that supervision needs to be a continuous, ongoing process, spanning over a significant period of time to monitor various data processing activities. It should become a regular and ongoing function of the DPAs, which must designate personnel solely responsible for supervising the large-scale IT systems working within specialised units on the systems to ensure continuity and the building of expertise. The personnel must be trained by the EU Fundamental Rights Agency (FRA) to acquire awareness of the various fundamental rights challenges and understanding on the specificities of the field of migration, asylum and border management. If assistance is needed from civil society, lawyers or academics this should be sought to improve the understanding of how interoperable systems operate, as this is not proscribed by the legal framework. Supervision should take place not only in relation to different data processing activities but also in the various *loci*; at the borders, on random immigration checks, in the visa authorities (including when these activities are delegated to private companies). Thus, supervision must become not only an ongoing activity, but also one on the ground to check in real-time how personal data are collected and processed at the borders, extraterritorially (for example when visa applications are lodged) and on national territory. This includes the need for close supervision by the EDPS of EU agencies and the role of CSC to exchange good practices, clarify unclear rules, flag potential issues that have arisen in practice in line with the legal instruments. Particularly, in the case of the EBCG Agency whilst has a distinct role in devising the algorithms for ETIAS and VIS, supervision is all the more necessary to encompass these matters. Of course, supervisory authorities should not hesitate to use the full extent of their powers that have been entrusted to them under the GDPR – as regards the use of the databases for administrative (migration) related purposes, or the LED as regards their use for law enforcement purposes. It is clear that such intense supervision needs substantial budget. Enforcing the relevant rules on resources is necessary and in view of the millions of Euros invested in the development of the large-scale IT systems, allocating resources at the EU level should also be considered as a possible reform. It is highly uneven and particularly worrisome that whilst millions of Euros are spent on the creation of highly sophisticated systems, it is not equally feasible to carve out a dedicated portion of their budgetary needs for recruitment, training and staffing needs of national supervisory authorities.

*c) The curious case of logs*

One of the key ways in which supervisory authorities can monitor the data processing activities is monitoring the data processing logs. Logs typically include the date and time of a data processing activity, the data used to perform a search, the data processed and the name of authorised staff or authority (and potentially the unique user identifiers of

both the competent authority and the person processing the data).[77] The retention period of logs differs: in the case of SIS it is three years, but can be kept for longer if required for monitoring procedures that are already underway.[78] In the case of VIS and EES, there is no clarity because the legal instruments refer to one another without specifying a retention period.[79] In the case of Eurodac, art. 52 of Regulation 2024/1358 is silent on the matter. For ETIAS, the logs must be deleted one year after the retention period of ETIAs data expires, if they are not required for monitoring procedures which have already begun.[80] The Interoperability Regulations envisage rules on keeping logs in relation to ESP,[81] sBMS,[82] MID and CIR,[83] also without a fixed retention period. The keeping of logs is useful, as they can promote transparency and lawfulness of processing of personal data and they can facilitate the supervisory work. They may also prevent unauthorised access. However, they are curse disguised as a blessing because in an interoperable network of large-scale IT systems the number of logs is expected to be in the billions, which makes it impossible to track data processing activities. They are also tools that by default can only operate *ex post*, which means that in the meantime, an individual whose personal data may have been unlawfully processed may have suffered adverse consequences. In light of the above, it is not unthinkable that DPAs explore the option of using AI tools themselves to cope with the exorbitant number of logs.

As a suggestion, supervision could follow the data flows by taking specific individuals' data to comprehend whether they have been collected lawfully and chiefly whether they have been processed in line with the underling rules of the systems. Another idea is to focus on the different users and track their processing activities to determine whether their processing activities raise concerns, e.g. regarding data quality issues, or unlawful processing (e.g. transfer of data) due to lack of awareness or disregard of the rules.

*d) Encompassing non-discrimination*

The lack of clarity as to whether and where AI is embedded provides an additional obstacle to effective supervision; without knowledge of whether and where exactly AI is, how can the "human over the loop" supervise? In *Ligue des droits humains*,[84] concerning the compatibility of the EU PNR Directive with fundamental rights, the Court referred to the necessary role of data protection officers and national supervisory authorities "to ensure

[77] Art. 12(2) Regulation 2018/1861 cit. and arts 22 and 34 Regulation 2021/1134 cit.
[78] Art. 12(3) Regulation 2018/1861 cit.
[79] Art. 46(2) Regulation 2017/2226 cit. and art. 34 Regulation 2021/1134 cit.
[80] Art. 69(4) Regulation 2018/1240 cit.
[81] Art. 10 Interoperability Regulations cit.
[82] Art. 16 Interoperability Regulations cit.
[83] Art. 36 Interoperability Regulations cit. and art. 24 Interoperability Regulations cit.
[84] Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministres* ECLI:EU:C:2022:491.

the monitoring of the lawfulness of the automated processing carried out by the [Passenger Information Unit] PIU".[85] The Court clarified that the monitoring covers among others whether those operations are not discriminatory. For this purpose, the data protection officer must have access to all data processed by the PIU, that access must necessarily cover the pre-determined criteria and databases used by that unit in order to guarantee effectiveness and a high level of data protection that that officer must ensure. Similarly, the investigations, inspections, and audits to be carried out by national supervisory authorities may also concern those pre-determined criteria and databases.

These pronouncements denote the value of the right to personal data protection as a right that can safeguard other fundamental rights, such as the right to non-discrimination.[86] This approach was signalled already in the CJEU judgment in *Huber* concerning an Austrian living in Germany who complained about his inclusion in a German database for foreigners that was much more comprehensive that any database on German nationals.[87] In his complaint, he claimed that he had been discriminated against on the basis of nationality. The CJEU analysed the facts through the data protection lens and considered discrimination within the data protection analysis.[88] The case could be seen as signalling the instrumental nature of data protection (and privacy), which would safeguard the different rights at stake by internalising them within its internal balancing/proportionality exercise.[89] Second, it elevates national supervisory authorities as guardians of non-discrimination through data protection law by opining that their investigations, inspections and audits may also concern those pre-determined criteria and those databases.

Data protection authorities must be equipped with personnel that is trained on the benefits and implications of the use of AI in general and in the field of migration, asylum and border management in particular, where the challenges for non-discrimination are heightened due to the inherently discriminatory nature of migration law as well as the potential vulnerability of foreigners. Otherwise, external expertise must be sought to complement the rich data-protection related expertise of the DPAs. Potential collaboration with the National Committee for Human Rights could be fostered as well, so that DPAs have a more individual-centric approach, as opposed to a more depersonalised solely data-centric one. Requiring from data protection authorities to have tasks relating to safeguarding non-discrimination may be a bit too much to ask of them. Given the emphasis of the CJEU to encompass non-discrimination within the role of the DPAs, they must have non-discrimination related trainings to understand the different challenges,

[85] *Ligue des droits humains* cit. para. 212.

[86] P De Hert and S Gutwirth, 'Data protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action' in S Gutwirth S, Y Poullet, P Hert, C Terwangne and S Nouwt (eds), *Reinventing Data Protection* (Springer 2009) 24-31.

[87] Case C-524/06 *Heinz Huber v Bundesrepublik Deutschland* ECLI:EU:C:2008:724.

[88] *Huber* cit. para. 66.

[89] R Gellert and S Gutwirth, 'The legal construction of privacy and data protection' (2013) Computer Law & Security Review 522-530.

the different types of biases at the design of algorithms and their implementation, the biases of the "human in the loop" ultimately responsible for the decision-making and the ways in which data protection can empower individuals who have been disproportionately discriminated against to exercise their rights under data protection law and seek judicial remedies.

The supervision conducted must concern all different forms of processing of personal data, including automated processing. However, the CJEU does not mandate how supervisory authorities should conduct their tasks, but rather allowed them discretion by investigating, inspecting or auditing the relevant pre-established criteria and databases. In *Ligue des Humains*, Advocate General Pitruzzella provided some additional insights into how supervision ought to take place noting that supervision must be "able to cover all aspects inherent in the automated processing", "including identifying the databases used to compare data [...] and to draw up the pre-determined criteria used for the analysis" and must take place both *ex ante* and *ex post*.[90] The temporal issue raised by the Advocate General is crucial and correlates with the earlier suggestion that supervision must be on the ground and an ongoing, continuous process in order to track the data flows and how these have affected and shaped the final decision-making.

There is another challenging issue concerning specifically the CRRS as a non-personal data database with statistical data and its supervision. Statistical data are anonymised data that will be drawn from the individual systems and stored in the CRRS pursuant to art. 39 of the Interoperability Regulations. Because they are anonymised, they do not qualify as personal data and therefore are not subject to EU data protection law, including the rules on supervision by national supervisory authorities and the EDPS. At the same time, art. 111 of the AI Act foresees that IT systems must be brought in line with its requirements by 2030. Given that the implementation of interoperable large-scale IT systems is expected to complete in 2027, this means that there is a three-year gap whereby the AI Act will apply, but not necessarily in relation to the IT systems, which will still have 3 more years for being brought in line with the AI Act requirements. The delay in applying the AI Act in the context of interoperable IT systems is highly problematic for an additional reason: as mentioned earlier, the CRRS is likely to use AI tools in the compilation of tailor-made, cross-system statistical data and analytical reporting for policy, operational and data quality purposes. Halting the application of the AI Act signifies that the supervision of AI tools at the national level, as envisaged in the AI Act aimed at ensuring accountability, is also delayed. The result will be that the CRRS will not be subject to any supervision, either from the perspective of EU data protection law or from the AI Act until 2030. This accountability gap is particularly significant; it means that for a number of years, the operation of this interoperability component will essentially become a black site. From 2030

[90] Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministres* ECLI:EU:C:2022:65, opinion of AG Pitruzzella, para. 229.

onwards, the supervision of AI systems will include the systems as well and will probably encounter additional difficulties through *ex post* conduct audits on the CRRS.

### IV.2. Harvesting the potential of the ETIAS and VIS Fundamental Rights Guidance Boards

The algorithmic profiling of applicants for travel authorisations and visas in ETIAS and VIS respectively is a particular case that merits further attention. There are two Fundamental Rights Guidance Boards set up with "an advisory and appraisal function",[91] composed of the Fundamental Rights Officer of the EBCG Agency and representative of the consultative forum on fundamental rights of the EBCG Agency, the EDPS, the EDPB and the FRA. The Boards must perform regular appraisals and issue recommendations to the ETIAS and VIS Screening Boards that will have advisory role in devising the ETIAS and VIS screening algorithms, a task, which as mentioned below, is entrusted to the ETIAS Central Unit. These recommendations concern the fundamental rights impact of ETIAS, in particular with regard to privacy, personal data protection and non-discrimination. The ETIAS and VIS Fundamental Rights Guidance Board shall also support the ETIAS Screening Board in the execution of its tasks when consulted by the latter on specific issues related to fundamental rights, in particular with regard to privacy, personal data protection and non-discrimination. They must have access to the audits carried out by the ETIAS Central Unit regarding the processing of travel authorisation and visa applications. This body did not feature in the Commission proposal and comes from a European Parliament suggestion for an Ethics Board.[92] However, the relevant provision was watered down and the Boards will not have any auditing role themselves. In any case, the involvement of representatives from the EDPS and the EDPB, which is composed of DPAs signifies that the supervisory role may be facilitated by obtaining inside knowledge into the workings of the ETIAS and VIS screening algorithms. The role of the Boards could be leveraged so that not only potential fundamental rights issues are prevented before they materialise by intervening at the design or deployment of AI, but could also provide insights for following up on specific issues that have emerged during the work of the Boards that could be followed up in more depth for example, through inspections and audits.

[91] Art. 10 Regulation 2018/1240 cit. and art. 9(l) Regulation 2021/1134 cit.

[92] Report COM(2016) 0731 – C8-0466/2016 – 2016/0357A(COD) of the European Parliament on the proposal for a regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399 and (EU) 2016/1624 42-43.

### IV.3. The AI Act's market surveillance authorities

Irrespective of the challenges and gaps regarding the classification of the interoperability components in line with the requirements of the AI Act, the latter provides for an enforcement system post-deployment whereby each Member State must designate a competent national authority – the so-called "market surveillance authorities". A market surveillance authority is defined by the AI Act as "the national authority carrying out the activities and taking the measures pursuant to Regulation 2019/1020".[93] The latter defines market surveillance as "the activities carried out and measures taken by market surveillance authorities to ensure that products comply with the requirements set out in the applicable Union harmonisation legislation and to ensure protection of the public interest covered by that legislation".[94] These authorities should have effective investigative and corrective powers, including at least the power to obtain access to all personal data that are being processed and to all information necessary for the performance of its tasks. The market surveillance authorities should be able to exercise their powers by acting with complete independence.[95] According to art. 74(8) of the AI Act, these authorities will be the DPAs, which have expressed such interest, and in any case the EDPS will act as a competent market surveillance authority in respect of AI systems deployed and used by EU institutions and bodies. The possible involvement of the DPAs is blessing and an anathema; in light of their existing experience with the operation of the IT systems the DPAs may have a better understanding of the fundamental rights issues at stake – although as mentioned earlier, this understanding must be broad enough, so that individuals are not viewed simply in terms of their personal data and that data protection related matters will not monopolise the interest. Furthermore, the efforts will not be duplicated either and continuity in supervision can be ensured. At the same time, the pathogenic features of supervision, particularly the lack of resources and relevant expertise, may remain, affecting the supervision capacity. The DPAs may not be adequately staffed or may end up overburdened and the supervisory tasks may be exercised in less depth than it is necessary. It is welcomed that where the high-risk AI system is intended to be put into service by immigration or asylum authorities the market surveillance authority must be notified.[96] Finally, it is also welcomed that the market surveillance authorities can be notified on incidents and malfunctioning not only by the providers notifications, but also by individuals who can lodge complaint, as this can mitigate power asymmetries, which in the field of migration, asylum and border management are heightened.

[93] Art. 3(26) AI Act cit.
[94] Regulation (EU) of the European Parliament and of the Council of 20 June 2019, art. 3(3)
[95] Recital 159 AI Act cit.
[96] Art. 43(1) AI Act cit.

## V. Conclusion: supervising interoperability as a mission impossible for the human over the loop?

This *Article* aimed to provide clarity into the interplay of interoperability and AI and highlight how this interplay will make the supervision of large-scale IT systems a very complex activity that cannot be done in the same manner as in the case of systems operating in silos. Reading behind the legislative instruments, it appears that interoperability continues to be the gift that keeps on giving; by integrating AI in the shadows of the AI Act makes it all the more necessary that the practical implementation needs proper monitoring. This is a first-class opportunity to rethink supervision, which is a constituent component of the right to data protection more holistically. Whilst supervision cannot replace the EU legislature, it can certainly bring clarity as to whether and to what extent the legislation is as problematic as academia has long warned and thus attract attention to the matters that need either legislative, judicial or policy intervention. This will be beneficial to give teeth to the right to personal data protection, included in the Charter, but nucleus and value has been debated over the years. This could be in line with the discussions about the value of data protection as safeguarding other rights and principles such as non-discrimination. Supervision should thus incorporate a broader understanding of fundamental rights and a more holistic approach. In this regard, an idea would be that data protection authorities are enriched with staff who have a background in the protection of fundamental rights.