

ALGORITHMISATION, ARTIFICIAL INTELLIGENCE (AI) AND THE RULE OF LAW IN EU IT LARGE-SCALE SYSTEMS

Niovi Vavoula*

ABSTRACT

This blog examines how the transformation of European border management in the era of algorithms and AI multiplies the rule of law challenges raised by ‘traditional’ digitalisation tools using the case study of EU large-scale IT systems. It also demonstrates the opaque nature of AI and the hidden potential of interoperability, a debate absent from the negotiations towards the adoption of the Interoperability Regulations. It is further argued that this opacity magnifies the obstacles faced by third-country nationals in obtaining meaningful information regarding the decision-making process behind their travel authorisation or visa application. The blog calls out a ‘rule of technology’ approach rather than a rule of law approach, which on the one hand creates the illusion of consistency and administrative efficiency, while in fact it erodes the rule of law.

TABLE OF CONTENTS: 1. Introduction. – 2. Automated Processing of Applications for Schengen Visas and Travel Authorisations. – 3. Facial Images: The Hidden Shift towards Facial Recognition – 4. Is the Multiple Identity Detector AI-powered? - 5. Conclusion

1. Introduction

* Associate Professor and Chair in Cyber Policy, University of Luxembourg.

In recent years, EU migration management is marked by the proliferation of automation tools of various complexity, aimed to exploit the full potential of large quantities of data collected. An ally in these efforts has been the exponential increase in computing power leading to the emergence of novel techniques, particularly algorithms, especially advanced ones, such as Artificial Intelligence (AI). In the field of [migration](#), AI has the potential to revolutionise the way states manage mobility, decision-making and foreign community integration. [AI promises](#) modernised identity checks and border controls, as well as expedited and [efficient](#) decision-making regarding visa or asylum applications, and residence permits. It can also be used for more efficient refugee resettlement to increase integration prospects, or for various risk assessments for example, to evaluate irregular migrants' or asylum seekers' [placement](#) in administrative detention. AI tools may also be used for more evidence-based policy-making through the prediction and prevention of influxes of refugees and migrants based on [predictive analytics](#); or for enhanced situational awareness around the borders by analysing surveillance footage collected by sensors deployed at states' frontiers and transforming it into actionable information and alerts for border and coast guard authorities.

This move is in line with a 'techno-solutionist' perspective, where technology is deemed neutral and as a panacea for the human incapacity in processing large amounts of data generated by other technological advents, coupled with increased human mobility – with Europe having become a '[global migration magnet](#)', requiring swift decision-making and, increased efforts to sift the *bona fide* travellers, migrants or refugees from the *mala fide* ones.

Whereas [research](#) in this area has been on the rise with a [focus](#) on the protection of fundamental rights, such as the principle of [non-discrimination](#), (also [here](#)), the rule of law challenges are relatively less researched (for example see [here](#) and [here](#)). As highlighted by Burgess, the rule of law has traditionally constrained the arbitrary exercise of power, however it has been deployed to limit *human* decision-making. This [questions](#) whether and how the rule of law can and should apply to *non-*

human decision-making. In his view, the modern rule of law is centred on explainability due to AI's inherent opacity. [Indeed](#), such tools are designed based on the end users' instructions to the developers, but the logic behind is opaque, and frequently proprietary. In this blog I aim to add to these [debates](#), by providing rule of law challenges stemming from the progressive shift towards AI-fication of European borders. I focus on the principles of legality, legal certainty, and the existence of effective judicial protection through access to judicial [remedies](#).

I apply them in the context of EU large-scale IT systems, considering that the extent to which AI is, or will be, embedded in these systems is unclear. Although Article 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', no legal instrument governing the IT systems or interoperability and no implementing or delegated act mention the term 'AI'. This delay in bringing the large-scale IT systems within the scope of the AI, coupled with Article 83 of the [Commission Proposal](#) for an AI Act which *ab initio* excluded them from the scope indicates that the IT systems are anticipated to rely on AI tools. But where exactly and how will it work is still uncertain.

In this blog, I explore the algorithmic reliance of large-scale IT systems aiming to show where AI can/will be by looking into algorithmic risk assessment, the deployment of facial recognition technology, and interoperability's interplay with AI. In the analysis, I identify specific rule of law challenges arguing that the lack of reference to AI creates significant foreseeability concerns. Thus, at EU level, the problem does not lie in the existence of law, but rather its *quality*, hindering foreseeability, as to the deployment of AI. Other rule of law challenges involve the inapplicability of the AI Act for some years, as well as the significant discretionary power provided to Frontex and eu-LISA, and the obstacles for individuals to meaningfully seek judicial remedies *ex post*. Let's see each of these issues in more detail.

2. Automated Processing of Applications for Schengen Visas and Travel Authorisations

2.1. Looking for AI and the Central Role of the CRRS

Regulations [2018/1240](#) on ETIAS and [2021/1134](#) on the revised VIS foresee the automated processing of applicants for travel authorisations and Schengen visas as a pre-empting control mechanism enabling extraterritorial border control. The ETIAS Regulation requires visa free travellers to apply online for travel authorisation before travelling to the Schengen area and disclosing a series of personal data which will be subject to automated checks against: (a) the other IT systems, Europol data and the Interpol databases, Stolen and Lost Travel Document database (SLTD) and the Interpol Documents Associated with Notices databases (TDAWN) – this cross-checking will be facilitated by the [European Search Portal \(ESP\)](#); (b) screening rules, in other words algorithms enabling profiling based on risk indicators; and (c) a dedicated watchlist of persons suspected of terrorist or serious crime. The revised VIS Regulation foresees similar rules on algorithmic profiling with some differences. For example, even if automated processing does not reveal any hits with other information systems or databases or algorithms, the visa application will be processed manually at national level and there is no automated positive decision-making.

Whereas automated processing of visa and travel authorisation applications against databases and the watchlist will assist in identifying known individuals, the screening rules, which will be developed by the ETIAS Central Unit, established in the EBCG Agency, aim to identify persons who are unknown to the competent national authorities. As [argued elsewhere with Karaïskou](#), both functions will rely on different types of algorithms; the first two functions are algorithm-reliant enabling data matching, the third type of automated processing relies highly on automation, involving [data mining](#). Flagging an applicant as potentially risky occurs because they display particular [traits](#) in a probabilistic logic

simply because other individuals, with whom applicants have common characteristics, had been deemed as constituting a risky profile.

The reference to the vague term ‘algorithm’ exemplifies the avoidance of the term ‘AI’. Even the term algorithm has been contested; Frontex has deemed it preferable to refer to filtering queries than algorithms, and that [no AI is involved](#) in the risk assessment. As [Zandstra and Brouwer](#) stress, this approach contradicts with the wording of the legal instruments and exemplifies the politics around the AI use.

According to [Karaïskou](#), 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’. An [eu-LISA report](#) states that CRRS collecting statistical data from VIS, EES and ETIAS of overstayers and information regarding refusals of entry of third-country nationals can use AI tools for risk-identification by recognising patterns from historical data analysis related to security, irregular migration and high epidemic risks. Furthermore, in the Future Group on Travel Intelligence and Border Management Report by [Europol and the EBCG Agency](#), it is stated that in cooperation with eu-LISA and other agencies, the joint analysis capability could leverage the full potential of CRRS as a data source for analytical purposes and develop analytical tools for risk-assessment with AI support.

Moreover, the algorithmic design and content are not foreseeable. The rules are not written in law, which only contains the categories of data used for their creation and therefore individuals could only vaguely understand the profiling process. Without clarity and foreseeability as to the nature, design and content of the risk assessment of travellers through the algorithm resonates with what Hildebrandt has referred to as ‘code-driven’ and ‘data-driven’ law, which contrasts with [written legal norms](#).

The use of AI in CRRS for determining and verifying the risk profiles [raises questions](#) regarding the application of the AI Act. Arguably, CRRS constitutes a high-risk AI system, as it assists in profiling travellers, thus it must be subject to safeguards on risk management, human oversight, pre-market conformity assessments, and post-market monitoring.

Furthermore, both providers and deployers need to register specific information of the high-risk AI systems in an EU database managed by the Commission and the Member State concerned. 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. Important information, such as the training data or a fundamental rights impact assessment, do not need to be entered. From a rule of law perspective, this is an important exception because it may perpetuate the lack of transparency and foreseeability regarding the AI use in ETIAS and VIS. With the phased integration of interoperable IT systems in the AI Act until 2030, another question lies in the supervision of CRRS, which is supposedly composed of non-personal data, thus potentially outside supervisory arrangements under data protection law.

2.2. Significant Discretionary Power to Frontex and eu-LISA

The principle of legality requires putting sufficient [limits](#) to the discretionary powers of public authorities. Whereas the Commission will specify the risks, it is for Frontex to establish the specific risk indicators, with both ETIAS and VIS Regulation allowing significant discretion to the Agency as they merely require that the specific risk indicators are (a) based on the Commission's risk specification; (b) consist of a combination of certain data categories; and (c) are targeted, proportionate and non-discriminatory, which say nothing as to 'how personal traits and data will be weighed against each other in the risk assessment'.

eu-LISA, the technical developer and manager of ETIAS and VIS and developer of the profiling software also enjoys considerable discretion. The only limitation on the developer is that the algorithm shall enable profiling by comparing risk indicators with data in the application file, without [design specifications](#). Private companies hired by eu-LISA are involved in the algorithmic development, raising additional foreseeability questions.

2.3. Lack of Effective Extrajudicial and Judicial Remedies

Specific groups of travellers are likely to be disadvantaged compared to others based on proxies of protected characteristics, resulting in indirect discrimination and a presumption of ‘guilt’. Furthermore, the principle of individualised assessment of applications and the duty to give reasons, a good administration requirement, enshrined in Article 41(2c) of the EU Charter of Fundamental Rights (CFR), may be compromised to the extent that adverse decisions are adopted based on such profiles (see [here](#)). Moreover, the automated “hits” produced by ETIAS or the revised VIS may impair independent human evaluation, as human decision-makers tend to interpret information through pre-existing biases, leading to automation bias or more likely selective algorithmic adherence (see [here](#), [here](#), and [here](#)).

In light of the above, seeking effective judicial remedies, in line with Article 47 CFR is paramount for the safeguarding of the rule of law. Article 47 applies to all individuals regardless of their nationality in so far as any right conferred to them by EU law, or in a situation governed by EU law, is adversely affected. This is mentioned in the Article 26(6) of the ETIAS Regulation and Article 9c(6) of the revised VIS Regulations, as well as the Visa Code, which provide for third-country nationals’ right to appeal against the refusal, annulment or revocation of travel authorisations or visas in the Member State that issued them according to its national law.

The CJEU has repeatedly highlighted the importance of the duty to provide reasons, which guarantees transparency of administrative [action](#) and the possibility for the affected person to lodge an [appeal](#). The reasons provided must be ‘[sufficiently specific and concrete](#)’ so that the person concerned can understand the grounds of the measure adversely affecting him. The statement of reasons must [disclose](#) the legal and factual reasons that led to the decision adoption in a clear and unequivocal [fashion](#). In [R.N.N.S and K.A.](#), the Court held that summary justifications based on pre-determined lists of grounds did not meet this threshold of specificity, as the statement of reasons must indicate the applicable ground, and the essence

of the reasons of the refusal. In *Ligue des droits humains*, on the processing of air passengers' Passenger Name Record (PNR) data, including via profiling, the CJEU underlined that Member States must ensure that the affected person can understand how those criteria and programs work, without necessarily disclosing to him/her what these are during the administrative procedure, so that he/she can 'decide with full knowledge of the relevant facts whether or not to exercise his or her right to [...] judicial redress'. The CJEU clarified that the competent national court and the person concerned, must have the opportunity to examine all the grounds and evidence based on which the decision was taken. This interpretation obliges the administration to provide meaningful information to the person concerned, along with the reasons, indicating that their personal data have been subjected to automated processing. The Court's interpretation also seems to imply the explanation of the algorithmic decision, including the types of personal data automatically processed and the rationale of the automated decision regarding the circumstances of the affected person.

In the case of ETIAS, Article 37 states that the pre-determined grounds for refusal are the following: use of a travel document is reported as lost, stolen, misappropriated or invalidated in SIS; the applicant poses a security, irregular immigration or high epidemic risk; the applicant is subject to a SIS alert; the applicant fails to reply to a request for additional information or documentation; the applicant fails to attend an interview or there are reasonable and serious doubts as to the authenticity of the data, the reliability of the statements made by the applicant, the supporting documents provided by the applicant or the veracity of their contents. Some of these grounds are concrete, for example, failure to attend an interview or to reply to a request for additional information within the deadline. Others are particularly vague, in particular that the applicant poses a security risk, an illegal immigration risk or a high epidemic risk. Without further explanation these statements mean little to individuals. It is highly likely that in case the applicant fits a risk profile and has been 'caught' by algorithmic profiling, the boxes ticked will be precisely the latter, thus preventing individuals from receiving meaningful information

about the reasons behind the refusal of their application, perpetuating the ‘black box’ effect and making the decisions incontestable.

The applicant will receive a standardised [form](#) for the refusal of the travel authorisation which replicates the grounds under Article 37. The form *requires* the ETIAS National Unit to fill in a free-text box as well with a mandatory statement of relevant facts and additional reasoning underlying the decision. The free text box cannot be left unfilled. However, it is unclear how this requirement will be implemented in practice and whether the individual will receive any meaningful information about whether it was an algorithm or a database that flagged them as a potentially risky applicant and in case of the former, any information about the criteria employed to seek remedies. Whereas the risk profiles will not be revealed, there is potential offered in the handbook foreseen in Article 93 of the ETIAS Regulation, aimed at providing any concrete guidelines on the implementation of ETIAS that could address such concerns.

In the case of VIS, whereby information and materials beyond the requirements of the VIS play a role, things are more complex. The revised VIS rules have led to zero changes in the information provided to rejected applicants. Annex VI of the [Visa Code](#) includes the standard form for refusal of visa applications, but it was not adapted to the introduction of algorithmic profiling through VIS. The form contains 17 boxes, each corresponding to one or more grounds set out in the Visa Code for refusing, annulling or revoking a visa. Four of these grounds may be used to refuse a visa application based on algorithmic profiling, namely where ‘one or more Member States consider you to be a threat to public policy or internal security’, ‘one or more Member States consider you to be a threat to public health’, ‘one or more Member States consider you to be a threat to their international relations’ and that ‘there are reasonable doubts as to your intention to leave the territory of the Member States before the expiry of the visa’. Without additional information on whether the decision is related to an algorithm, the refused applicant will have significant difficulties understanding the underlying reasons behind the refusal. Although there is a section on ‘additional remarks’, this does not appear to be mandatory by visa authorities. A useful case in this respect is [R.N.N.S. and K.A. v](#)

[*Minister van Buitenlandse Zaken*](#), whthe CJEU explained that in cases of objections to granting a visa, the identity of the Member State(s) that objected to the issuing of a visa and the specific ground for refusal based on that objection, accompanied, by the essence of the reasons for that objection, must be provided.

3. Facial Images: The Hidden Shift towards Facial Recognition

The legal framework of large-scale IT systems is equally confusing as to the use of AI in the processing of biometric data, namely fingerprints and facial images. Except for ETIAS, IT systems process different types of biometric data, with emphasis on verification and identification initially through fingerprints and facial images. Fingerprint identification [already occurs](#) in Eurodac, VIS and SIS to identify third-country nationals at the borders or on national territory. There is also urge in making the most of facial images, through the deployment of facial recognition technology (FRT), which is more invasive. All EU large-scale systems, except ETIAS, already process or will process facial images.

[Regulation 2017/2226](#) on EES foresees two types of biometric identifiers - four fingerprints and a facial image - and has provided for the use of FRT for verification purposes at the border and on national territory. EES relies on machine learning techniques for biometric matching. Facial images may also be used combined with fingerprints to identify individuals and border or immigration authorities shall have access to search with the fingerprint data or the fingerprint data combined with the facial image, for identifying third-country nationals being registered previously in EES under a different identity or not fulfilling the entry or stay conditions of the Member States.

[Regulation \(EU\) 2024/1358](#) on the revised Eurodac foresees the recording of facial images alongside fingerprints regarding individuals falling within the personal scope of the database. Both fingerprints and facial images are

to be used for comparison to maximise high degree of accuracy in identifying individuals.

Articles 22-23 of the [2018 SIS framework](#) regulate the processing of photographs, facial images and dactyloscopic data fulfilling minimum data quality standards and technical specifications and must be processed following a [data quality check](#). Facial images will not only be used to confirm the identity of a person, but also as soon as it becomes technically possible facial images may be used to identify a person within regular border crossing points.

Similarly, Article 6 of the [ECRIS-TCN Regulation](#) foresees that in the first stage, facial images may be used only to confirm the identity of a third-country national who has been identified due to alphanumeric fingerprint search. In the second stage facial images will be used to identify third-country nationals to determine the Member States holding information on previous convictions concerning them.

Finally, in the revised VIS Regulation [Article 22a(1)(j).], the collection of live facial images is foreseen during the application process to enable biometric matching using facial recognition technology. Furthermore, in rules mirroring the EES Regulation [Article 18 revised VIS Regulation], facial images will be used to verify the identity of a visa holder at the borders or to identify them in combination with their fingerprints. However, it is stated in Article 20 of the revised VIS Regulation that facial images shall not be the only search criterion.

The legal instruments make *no single reference* to the FRT, leaving the reader to guess about the tools deployed, but eu-LISA clearly [speaks about](#) FRT. The legal landscape becomes even more convoluted with the Interoperability Regulations, which foresee the creation of a shared Biometric Matching Service (sBMS), which will store biometric templates of all the biometric data stored in the underlying IT systems. sBMS plays a pivotal role in deploying FRT using the biometric data stored in the IT systems, but this does not flow from the legal framework, either the legislation or the delegated acts. It is rather confirmed by eu-LISA [itself](#). In the case of EES, [eu-LISA](#) further states that the system will rely on machine learning techniques for biometric matching. In the case of [SIS](#), the

processing of facial images will occur 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’.

The lack of foreseeability does not concern only the type of technologies used for the performance of certain tasks, but also the uses of this technology. Biometric data will be used for biometric recognition, including verification and identification. However, in the case of SIS, things are far more complex. According to Article 33(4) of [Regulation 2018/1861](#), biometric recognition occurs first to identify a person and ‘as soon as it becomes technically possible, and while ensuring a high degree of reliability of identification’ facial images may be used to identify a person within regular border crossing points.

4. Is the Multiple Identity Detector AI-powered?

Another example of how interoperability conceals the potential recourse to AI systems concerns the operation of Multiple Identity Detector (MID). The latter involves the cross-checking of personal data of third-country nationals on a continuous basis (on border crossing, on identity checks, on automated risk assessments etc) 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 Article 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, regarding alphanumeric data, searches in ESP will occur using different combinations of certain biographical data or travel document [Articles 27(3)-(4) of the Interoperability Regulations]. 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, [Delegated Regulation](#)

[\(EU\) 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. To that end, the Delegated Regulation provides an exhaustive list of rules for when identity data shall be considered as similar. [These rules](#), known transliteration of names, inversions of name and surname, cases of letter order, or differences due to hyphens, inversion of date and month. 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’. eu-LISA must monitor the impact of the application of the algorithm and report, to the Expert Group. Where necessary, to limit the number of cases in which yellow links generated by the MID would need to be turned into white links the Commission shall request eu-LISA to adjust the algorithm by prioritising the yellow links created between identity data that are considered more similar. It cannot go unnoticed that once again the Delegated Decision uses the term ‘algorithm’ without specifying whether it falls under the definition of AI. This marks another instance of inherent opacity of the inner workings of MID through law, which generates lack of foreseeability as to the nature of MID and challenges the legality principle. The omission of the legislation is coupled with deliberate lack of specificity through the use of a vague term in the delegated act.

5. Conclusion

This blog aimed to highlight how the transformation of European border management in the era of algorithms and AI multiplies the rule of law challenges raised by ‘traditional’ digitalisation tools due to opacity in the nature of the algorithms employed. This secrecy and opacity creates confusion through terminological ambiguities and potentially downgrades the importance of the shift towards algorithmisation, hinders democratic scrutiny, avoids legal obligations and ultimately shrinks the protection

offered to the individuals affected. The use of the more neutral term ‘algorithm’ as a form of technological neutrality shifts the attention from the more loaded term AI and/or leaves flexibility for the deployment of AI. This blog demonstrated the true, hidden potential of interoperability, a debate which did not feature *at all* in the negotiations towards the adoption of the Interoperability Regulations. Such a blunt disregard for the rule of law via concealing that interoperability components are *pre-requisites* or *motors* for the deployment of AI is particularly significant, exemplified also via the temporary exclusion of interoperable IT systems from the scope of the AI Act. The blog also demonstrated

the obstacles faced by different groups of third-country nationals in obtaining meaningful information regarding the decision-making process behind their travel authorisation or visa application and therefore seeking judicial protection will be particularly obstructed; after all, if individuals do not know what went wrong with their application, how can they challenge it? A ‘rule of technology’, rather than a rule of law approach has thus emerged, whereby technical feasibility dictates the legal and policy developments in an opaque manner, which creates the illusion of consistency and administrative efficiency, where it actually erodes the rule of law and leaves third-country nationals at its margins.

To cite this contribution: N. VAVOULA, *Algorithmisation, Artificial Intelligence (AI) and the Rule of Law in EU It Large-Scale Systems*, ADiM Blog, September 2026.