Will AI 'subtly' take over decision-making in the EU migration context? Warnings and lessons from ETIAS and VIS

Lorenzo Gugliotta*,[1] Abdullah Elbi[2]

Katholieke Universiteit (KU) Leuven, Centre for IT & IP Law (CiTiP), Leuven, Belgium
**Corresponding author*: lorenzo.gugliotta@kuleuven.be

Abstract

In 2019 the EU laid down the regulatory groundwork for the ambitious 'Interoperability' project in the Area of Freedom, Security and Justice. To make detection and analysis more effective, interoperability will rely significantly on automated processes. The algorithmic tools enabling these processes can qualify as 'AI systems' under the proposed AI Act, which seeks to protect individuals against undesirable effects of AI, such as undue interferences with fundamental rights. However, AI tools used by interoperable migration databases are excluded from its scope based on the current text. In this paper, we focus on the use of AI technologies in the envisaged interoperability framework as complicating factor for balancing security objectives and fundamental rights. As a case study, we focus on the AI-enabled processing envisaged under ETIAS and VIS to clear third-country nationals applying for a travel authorisation or a Schengen visa, respectively. This processing was conceived to merely facilitate and guide the decision by national authorities and avoid taking decisions based solely on automated means; however, we argue that ETIAS and VIS might hide risks such as favouring de facto *AI-based profiling, engendering informal 'rulebooks', and progressively reducing the extent to which human reviewers question the AI-generated recommendations. Relying on the existing EU data protection rules, we therefore investigate whether ETIAS and VIS provide sufficient safeguards and define clear responsibilities to prevent exposure of third-country nationals to decisions based solely on automated means. By analysing the implications of the AI-enabled processing already envisaged in the current EU border regulation, the paper seeks to draw useful lessons for further adoption of AI in the border and security ecosystem.*

Introduction

Automation, notably achieved via artificial intelligence ('AI') technologies, is gaining traction in virtually all areas of government intervention.[3] Border and migration control are no exception.[4] From a functional perspective, automation and AI are particularly suited to handling the high amount and

[1] Lorenzo is a legal researcher at Katholieke University Leuven (Belgium) – Center for IT and IP Law (CiTiP) where he carries out research on the relationship between artificial intelligence, automation and the law, particularly fundamental rights and data protection.

[2] Abdullah is a legal researcher at Katholieke University Leuven (Belgium) – Center for IT and IP Law (CiTiP) where he studies the use of AI-based biometric technologies in the security domain and is primarily involved in the Horizon 2020 project iMars and the Research Council of Norway-funded SALT Project.

[3] See European Commission, AI Watch Artificial Intelligence in public services. Overview of the use and impact of AI in public services in the EU, Science for Policy Report, 2020, available at: https://joinup.ec.europa.eu/collection/elise-european-location-interoperability-solutions-e-government/document/report-ai-watch-artificial-intelligence-public-services-overview-use-and-impact-ai-public-services.

[4] See OECD, "The Use Of Digitalisation And Artificial Intelligence In Migration Management", February 2022, available at https://www.oecd.org/migration/mig/EMN-OECD-INFORM-FEB-2022-The-use-of-Digitalisation-and-AI-in-Migration-Management.pdf

variety of data and the time constraints that border and migration control entail.[5] All over the world, countless initiatives have integrated automation and AI technologies into border policies. They can be used in different settings – such as in *ex-ante* traveller vetting procedures and risk assessments,[6] border checks on departure and arrival, including biometric processing[7] – and with varying degrees of sophistication and human oversight. Ever since the 2013 European Commission's Smart Borders Package,[8] the EU has recognised the potential of automation in the border context. It embarked on a modernisation programme of the whole EU border management landscape, resulting in a batch of new large-scale information systems embedded in an interoperability architecture.[9]

Within this landscape, in this paper we focus on two EU information systems: the Visa Information System ('VIS'), operational since 2011, and the soon-to-be operational European Travel Information and Authorisation System ('ETIAS'). ETIAS and VIS are the two main tools for handling legal inbound migration flows into the Schengen area. The focus is on ETIAS and VIS for two reasons: first, they integrate AI-enabled traveller pre-screening and risk assessment capabilities that are particularly intriguing from a fundamental rights perspective; and secondly, they are going to deploy such capabilities based on enormous amounts of personal data of third-country nationals ('TCNs'). The data processing operations entailed by the ETIAS and VIS automated processing concern a series of data capable of directly identifying natural persons, including biometric data (only in VIS) and special categories of personal data, in particular data related to health. Moreover, the capability of these EU information systems of cross-checking such data with data contained in other systems under the interoperability architecture, makes these data processing operations all the more extensive and, potentially, invasive. EU fundamental rights watchdogs, in particular the European Data Protection Supervisor ('EDPS') and the Fundamental Rights Authority ('FRA'), and legal scholars pointed out such concerns when criticising the Commission for not carrying out fully-fledged fundamental rights impact assessments prior to launching the legislative procedures for the ETIAS, Interoperability, and VIS Recast Regulation.[10]

This paper focuses on one specific concern, i.e., the possible undesired effects of ETIAS and VIS algorithmic decision-making on the meaningfulness and effectiveness of human oversight over individual decisions on applications for travel. In order to do that, we assess the extent to which the

---

[5] See Ozkul, D., 2023. *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*. Oxford: Refugee Studies Centre, University of Oxford. © Algorithmic Fairness and Asylum Seekers and Refugees (AFAR) Project, and the Refugee Studies Centre, University of Oxford, 2023.

[6] For instance, AI-based risk analysis methodologies (to be) used by the European Border and Coast Guard Agency ('EBCGA' or 'Frontex'), see Frontex, *Artificial Intelligence Based Capabilities for the European Border and Coast Guard*, Final Report, 2021. These systems include also 'lies detectors', such as the Automated Virtual Agent for Truth Assessments in Real-Time ('AVATAR') deployed in the United States, see: https://discernscience.com/avatar/.

[7] These include tools relying on traditional biometrics, such as fingerprints and facial images; but also tools advancing the already existing biometric systems against identity fraud at borders. See the 'iMars' Project which aims to strengthen the security and robustness of facial recognition technology ('FRT') systems, see: https://imars-project.eu/

[8] Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security (COM/2016/0205 final).

[9] The goal of interoperability is to make EU borders more secure by increasing the number of cross-checks across data collected and stored in various databases. It was established by Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa; and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration.

[10] Zandstra, T.; Brouwer, E., *Fundamental Rights at the Digital Border: ETIAS, the Right to Data Protection, and the CJEU's* PNR *judgment*, VerfBlog, 2022, p. 3, available at: https://verfassungsblog.de/digital-border/; EDPS, Opinion 3/2017 on the European Travel Information and Authorisation System (ETIAS), 7 March 2017, para. 13, p. 7, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/european-travel-information-and-authorisation-system_en

ETIAS and VIS automated processing are captured by the prohibitions to automated decision-making in EU data protection law. We focus specifically on Article 22 GDPR and Article 24 of Regulation 2018/1725[11] (the EU Data Protection Regulation, hereinafter 'EUDPR'). This is because the personal data processing operations at hand are carried out either under the responsibility of EU bodies (i.e., Frontex, or Frontex jointly with eu-LISA), or under the joint responsibility of Frontex and the Member States.[12]

To date, the fundamental rights implications of border control and migration systems have received attention from EU bodies as well as scholars. The EDPS and the FRA have issued several opinions on the data protection and fundamental rights implications of the Smart Borders package,[13] interoperability,[14] as well as ETIAS,[15] the Entry/Exit System ('EES'),[16] VIS[17] and the Schengen Information System ('SIS')[18] individually. In terms of recent scholarly publications, Brouwer (2020)[19] assessed the necessity and proportionality of EU interoperability for borders and migration under data protection law; Blasi Casagran (2021)[20] focused on the challenges for various fundamental rights stemming from making EU border systems 'interoperable'; Vavoula (2021)[21] examined the fundamental rights implications of deploying AI systems at the EU borders; Zandstra and Brouwer (2022)[22] critically assessed the impact of ETIAS on the fundamental right to data protection; and most recently, Quintel (2022)[23] carried out a study connecting various data protection frameworks and their applicability to the EU borders and migration ecosystem; Derave, Genicot, Hetmanska (2022)[24] took the ETIAS automated processing as a case study to demonstrate their potential discriminatory effects; in the same vein, Eklund (2022)[25] discussed a wider array of challenges linked to the ETIAS automated processing. A lively literature can also be found on the prohibition of automated decision-making

[11] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[12] Pursuant to Article 56 ETIAS Regulation and Article 36a VIS Regulation.

[13] EDPS, Opinion 06/2016 on the Second EU Smart Borders Package ('SBP'), Recommendations on the revised Proposal to establish an Entry/Exit System, 21 September 2016, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/eu-smart-borders-package_en.

[14] FRA Opinion, Interoperability and fundamental rights Implications, 18 April 2018, available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-01-2018-interoperability_en.pdf.

[15] EDPS, Opinion 3/2017, cited *supra*, note 10; FRA Opinion 02/2017, The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS), 10 July 2017, available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-opinion-02-2017-etias.pdf.

[16] EDPS Opinion on the SBP and the revised EES proposal, cited *supra*, note 13.

[17] EDPS Opinion 9/2018 on the Proposal for a new Regulation on the Visa Information System, 12 December 2018, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/upgrading-visa-information-system-vis_en; FRA Opinion, The revised Visa Information System and its fundamental rights implications, 7 September 2018, available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-visa-information-system-02-2018-corr_en.pdf.

[18] EDPS Opinion 7/2017 on the new legal basis of the Schengen Information System, 2 May 2017, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/schengen-information-system-new-legal-basis_en.

[19] Brouwer, E., *Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection*, European Public Law 26, No. 1 (2020): 71-92, 2020 Kluwer Law International BV, The Netherlands.

[20] Blasi Casagran, C., *Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU*, Human Rights Law Review, 2021, 21, 433-457.

[21] Vavoula, N., *Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism*, European Journal of Migration and Law, 23 (2021) 457-484.

[22] Zandstra, T.; Brouwer, E., cited *supra*, note 10.

[23] Quintel, T., *Data Protection, Migration and Border Control: The GDPR, the Law Enforcement Directive and Beyond*, Hart Studies in European Criminal Law, Hart Publishing, 2022.

[24] Derave, C.; Genicot, N.; Hetmanska, N., *The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System*, European Journal of Risk Regulation (2022),13, 389–420.

[25] Eklund, A. M., *Frontex and 'Algorithmic Discretion'*, 2022, available at: https://verfassungsblog.de/frontex-and-algorithmic-discretion-part-i/.

under the GDPR. For instance, Veale and Edwards (2018)[26] critically assessed the 29WP Guidelines on Article 22 GDPR; González and de Hert (2019)[27] discussed that provision in connection with GDPR-based lawful grounds for processing; Malgieri (2019)[28] focused on the safeguards for data subjects, especially in terms of explainability of decisions; Sancho (2020)[29] provides an in-depth analysis of Article 22 gauged towards enhanced protection of individuals; and de Hert and Lazcoz (2021)[30] sought to 're-purpose' Article 22 within a more dynamic human oversight ecosystem vis-à-vis automated decision-making.

This article is structured as follows. Section I presents the role of ETIAS and VIS within the EU border migration and control architecture, describes the ETIAS and VIS automated data processing that will be the focus of the paper, and discusses if they qualify as AI. Section II analyses the ETIAS and VIS automated processing vis-à-vis the relevant prohibitions against decisions based solely on automated means, and explores whether the legal bases for the two instances of automated processing provide sufficient safeguards for data subjects. Section III provides concluding remarks.

Section I – AI in the EU Large-Scale Information Systems: The Case of ETIAS and VIS

This section briefly describes the objectives and role of ETIAS and VIS within the Schengen Area's migration and border infrastructure; then it describes separately the automated data processing entailed by ETIAS and VIS in the workflow potentially leading up to the granting of the travel authorisation or visa to the potential traveller. Based on this description, we then apply the definition of 'artificial intelligence (AI) system' as currently laid down in the proposed AI Act[31] to determine whether the ETIAS and VIS automated processing would qualify as AI system.

ETIAS and VIS within Interoperability

ETIAS and VIS are two information systems in the Area of Freedom, Security and Justice created, along with other systems, to implement and contribute to national and EU migration, border control and internal security policies. The 'younger' of the two systems, ETIAS was established in 2018 with Regulation 2018/1240[32] and, according to eu-LISA's latest plans, is set to enter operations in 2024.[33] ETIAS can be thought of as a European equivalent to the US 'ESTA' (Electronic System for Travel Authorisation). Designed to digitalise and modernise EU's migration policy, it is set to collect and process the data of visa-exempt third-country nationals (VE-TCNs)[34] who intend to travel to the

[26] Veale, M.; Edwards, L., *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, Computer Law & Security Review 34 (2018) 398-404.

[27] Gil González, E.; de Hert, P., *Understanding the legal provisions that allow processing and profiling of personal data – An analysis of GDPR provisions and principles*, Academy of European Law (ERA) Forum (2019) 19:597–621, available at: https://doi.org/10.1007/s12027-018-0546-z.

[28] Malgieri, G., *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, Computer Law & Security Review 35 (2019), 105327.

[29] Sancho, D., *Automated Decision-Making under Article 22 GDPR: Towards a More Substantial Regime for Solely Automated Decision-Making*, in Ebers, M. and Navas, S. (eds), *Algorithms and Law*, Cambridge University Press, 2020.

[30] De Hert, P.; Lazcoz Moratinos, G., *Radical rewriting of Article 22 GDPR on machine decisions in the AI era*, European Law Blog 2021, available at: https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/.

[31] The paper will rely on the latest publicly available compromise text of the AI Act. The version relied on was the General approach of the Council of the EU to the AI Act proposal, 25 November 2022, available at: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf.

[32] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.

[33] See 'Why was ETIAS delayed again to 2024?', available at: https://etias.com/articles/why-was-etias-delayed-again-to-2024.

[34] The determination of whether citizens of a given country are exempt from the requirement to hold a visa to enter the Schengen Area is based on Regulation (EU) 2018/1806. Annex I to that Regulation lists the countries whose citizens are required to hold a visa (VH-TCNs); Annex II list the countries whose citizens are exempt (VE-TCNs).

Schengen Area for a short term. VIS, on the other hand, has a much longer history than ETIAS. Established in 2004,[35] it entered operations in 2011, and since then it has collected and processed the data of visa-required (or 'visa-holding', VH-TCNs) travellers applying for short-term Schengen visas. VIS is based on Regulation 767/2008,[36] which was subsequently reviewed and recast on several occasions including the 2021 VIS Recast,[37] which enlarged the scope of the VIS to include long-stay visas and residence permits.[38] ETIAS and VIS together form the backbone of the IT infrastructure to manage short-stay inbound and outbound legal migration flows in the Schengen Area. Thanks to its much more recent conception, ETIAS was developed 'Interoperability-ready', i.e., already set to be integrated within the EU's Interoperability framework for migration and border management aimed increase the security of the EU via faster checks as a response, inter alia, to the terrorist threat.[39] VIS underwent technical and legislative amendments to be integrated into the Interoperability framework, including an automated processing of data mirroring the logic and – to some extent – the steps of the ETIAS automated processing.

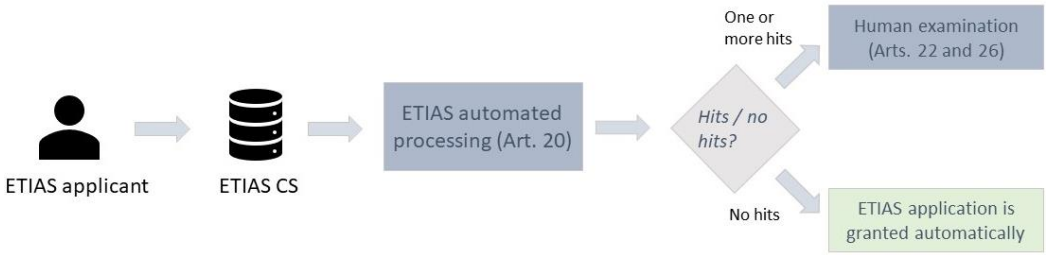
ETIAS and VIS automated processing

Both ETIAS and VIS will support automated data processing to analyse the risk profile of TCNs for the purpose of eventually granting or refusing a travel authorisation or visa. The automated processing of ETIAS and that of VIS share much of the logic but differ essentially in terms of a) the expected output and consequences of the automated processing; and b) the timing, role, and influence of manual processing.

Under the ETIAS Regulation, once it receives a new application by a TCN and records the applicant's data, in a first step the ETIAS Central System will execute the comparisons and analysis laid down in Article 20(5) of the ETIAS Regulation. These include essentially verifying, through the Interoperability components, whether the applicant's data match (in full or in part) data stored in other information systems and databases, including databases on convicted criminals and security alerts on specific persons, analysing the applicant's replies to the ETIAS application form, and applying screening rules and risk indicators to the applicant's data (see more on this below).[40] The second step concerns the outcome of this comparison: for any match found during the first step, ETIAS will create a 'hit', i.e., will flag the existence of a match or an outcome that should be analysed further. The transition from the second to the third step involves a binary question: if no hits are created, in the third step ETIAS will automatically grant the applicant an electronic travel authorisation with no human involvement; if, by contrast, one or more hits are created, in the third step the application file is up for manual processing pursuant to Articles 22 and 26 of the ETIAS Regulation, which will lead to a decision to grant or refuse the travel authorisation. The figure below helps visualising the ETIAS decision-making workflow.

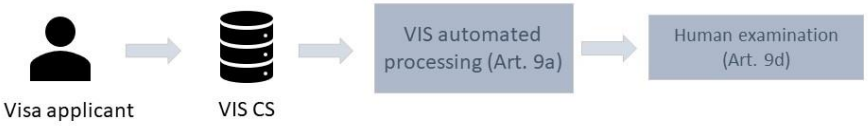
Figure 1: ETIAS workflow

[35] 2004/512/EC: Council Decision of 8 June 2004 establishing the Visa Information System (VIS).
[36] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas.
[37] Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System.
[38] From the time when the EES is in operation, VIS will switch to the shared Biometric Matching System (sBMS) which is an automated multi-biometric identification system for third-country nationals (non-EU/EEA/Swiss citizens) which will serve several systems (VIS, SIS II, Eurodac, EES, ETIAS and ECRIS-TCN). See further, eu-LISA, *Report on the technical functioning of the Visa information System (VIS)*, August 2022, available at https://www.eulisa.europa.eu/Publications/Reports/2021%20VIS%20Report.pdf
[39] See the Commission's Proposal for the Interoperability Regulations, COM(2017) 793 final – 2017/0351 (COD), p. 3.
[40] The list of comparisons to be carried out by the ETIAS Central System is laid down in Article 20(5) ETIAS Regulation.



The VIS process is similar but different. Upon recording the visa applicant's data, in a first step the VIS Central System will engage in a set of comparisons such as those provided for under ETIAS, essentially verifying whether the applicant's data match any data stored in other information systems and databases, and apply the same risk indicators as under ETIAS to the application file. In a second step, VIS will create hits for any matches. Regardless of whether any hit is created, the visa application file will be manually reviewed by the competent visa authority with a view to deciding whether to grant a visa or not. The figure below helps visualising the VIS decision-making workflow.

Figure 2: VIS workflow



For our purposes, the key difference between the ETIAS and VIS processes concerns the role of human reviewers (authorities). Whereas the system itself is authorised to issue a travel authorisation in the 'no-hit' scenario under ETIAS, and forced to revert to human review if one or more hits are triggered, the visa framework always entrusts the competent authority with issuing a visa. This distinction leads to a few terminological comments. Within a workflow, we qualify as 'non-final outcomes' those outcomes that, while leading to a tangible result, do not represent the outcome of the final step in the process. An example is the risk profile elaborated by the ETIAS CS after one or more hits are triggered: it is a tangible result, but does not end the process since the ETIAS NU and CU are going to step in. We then qualify as 'final outcomes' the outcomes produced at the end of the workflow, such as the human decision to issue or deny a travel authorisation or visa, or the decision by the ETIAS CS to issue a travel authorisation. These terms will be used further below.

The difference between the ETIAS and VIS workflow, and in particular in the powers assigned to the machines, stems from the different average risk profile that VE-TCNs and VH-TCNs are believed to carry from a migration and security policy perspective.[41] The automated screening is conceived as a first security filter on the application: if the ETIAS applicant passes the first screening, it is believed to pose no risk warranting human review; conversely, even if a visa applicant passes that first screening, a comprehensive human review of his or her case is still deemed necessary, and the automated processing is thought of as merely supportive or preparatory for the subsequent analysis by the authority.

With reference to the existing literature on automated support to decision-making, we follow the categorisation proposed by Binns and Veale,[42] the ETIAS case would belong to the 'triaging' category,

[41] See implicitly Recital 9 of the ETIAS Regulation.

[42] Binns, R.; Veale, M., *Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR*, International Data Privacy Law, 2021, Vol. 11, No. 4.

i.e., automated processes that are capable of 'labelling' a given individual and, for one or more of these labels, taking a direct decision concerning that individual, whereas the other labels would prompt the system to assign the case to a human caseworker.[43] In ETIAS the labelling is implicit, in that those applicants who do not trigger any hits in the automated process, whilst not assigned a formal label (e.g., 'green'), are still clustered as those applicants for whom an automated decision (to issue the travel authorisation) is taken with no human involvement. Conversely, the VIS case would belong to the 'decision support' category,[44] because any outcome of the automated processing (i.e., whether hit or no-hit) needs to result in human intervention to further the analysis and reach a decision.

Here it is appropriate to make one key terminological remark. By 'automated processing' (under ETIAS and VIS) we refer to the sequence of data processing operations whereby the two systems compare various data inputs with pre-defined conditions embedded in the systems' software, all the way to the output of that processing. In other words, we refer to the second step mentioned in the above description and highlighted in the two figures. It is key to point out that this paper does *not* focus on the entire ETIAS and VIS automated processing. As we saw above, such processing includes operations such as determining whether the applicant is a minor,[45] whether he or she has replied affirmatively to certain questions,[46] or whether he or she has data recorded in other information systems.[47] Operations such as these are *not* the focus of this research insofar as, taken individually, they do not require the system to utilise any 'intelligence' or decisional autonomy; by contrast, where the research *does* focus is on a subset of the whole automated processing, i.e., those specific data processing operations, whereby the system is expected to apply certain criteria and indicators to the individual situation of a data subject and derive non-trivial outcomes from it. This is the case of the following two provisions:

- Article 20(5) ETIAS Regulation, which reads: "The ETIAS Central System shall compare the relevant data referred to in points (a), (aa), (c), (f), (h) and (i) of Article 17(2) to the specific risk indicators referred to in Article 33."; and
- Article 9(a)(13) of the VIS Recast Regulation, which reads: "The VIS shall compare the relevant data referred to in point (4)(a), (aa), (g), (h), (j), (k) and (l) of Article 9 to the specific risk indicators referred to in Article 9j."

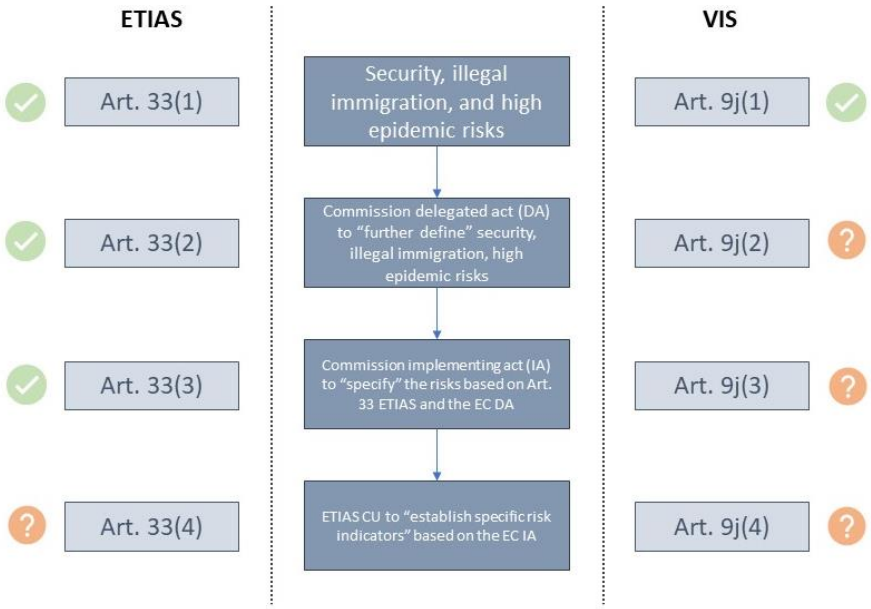
According to these two provisions, which mirror one another, ETIAS and VIS will compare the applicants' data to indicators regarding the security, illegal immigration, or high epidemic risk ETIAS and visa applicants may pose.[48] The indicators shall be established by the ETIAS CU (Frontex) based on a complex series of generic and specific risks. The high-level risks – i.e., security, illegal immigration, high epidemic risk – are already in the ETIAS Regulation; the Commission then needs to further define these risks via a delegated act,[49] which was adopted in 2021;[50] subsequently, the Commission shall, via an implementing act, specify the risks mentioned in the ETIAS Regulation and those defined in the delegated act;[51] finally, the ETIAS CU shall use all these regulatory sources to establish the risk indicators[52] to be used by the ETIAS screening rules. An identical method was introduced into the VIS Regulation: Starting from the security, illegal immigration, high epidemic risk, the Commission needs

[43] Ibid., p. 322-323.
[44] Ibid., p. 322.
[45] E.g., Article 20(2)(m) ETIAS Regulation.
[46] E.g., Article 20(3) ETIAS Regulation.
[47] E.g., Article 20(2) ETIAS Regulation.
[48] Cfr. Articles 33 ETIAS Regulation and 9j VIS Recast Regulation.
[49] Article 33(2) ETIAS Regulation.
[50] Commission delegated decision of 23 November 2021 on further defining security, illegal immigration or high epidemic risks. C(2021) 4981 final.
[51] Article 33(3) ETIAS Regulation.
[52] Article 33(4) ETIAS Regulation.

to adopt a delegated act[53] and subsequently an implementing act[54] to enable Frontex to develop the VIS specific risk indicators.

The figure below illustrates this sequence distinguishing the steps that have been completed from those yet to be taken.

Figure 3: ETIAS screening rules – Sequence of acts to be adopted



To date, the Commission has adopted the delegated act referred to in Article 33(2) ETIAS and the implementing act referred to in Article 33(3) ETIAS. On 2 June 2021, the EDPS published its formal comments to the draft ETIAS implementing act.[55] EDPS also published its formal comments on the draft VIS delegated act[56] and implementing act,[57] but neither is publicly available to date.

How will the ETIAS and VIS automated processing work in practice?

The legal groundwork of the ETIAS screening rules and the technical work on the algorithm are not yet complete; because of this, and due to confidentiality of information, it is not possible at this stage to provide a thorough account of the logic behind and the possible implications of the ETIAS screening rules and the related algorithm.

The ETIAS delegated act pursuant to Article 33(2) of the Regulation states that the analysis based on the statistics referred to in Article 33(a) to (f) should "result in sets of characteristics of specific groups of travellers associated with security or illegal immigration or high epidemic risks. The interpretation of these sets of characteristics will make it possible to identify specific risks. These will, in turn, form the basis for the development of specific risk indicators."[58] The act then defines 'sets of characteristics'

[53] Article 9j(2) VIS Regulation, as amended by Regulation (EU) 2021/1134.
[54] Article 9j(3) VIS Regulation, as amended by Regulation (EU) 2021/1134.
[55] EDPS Formal Comments on the draft Commission implementing decision on specifying the risks as defined in Regulation (EU) 2018/1240 as well as in the Commission Delegated Decision [TBD] [Delegated Act], available at: 2021-0404_d1140_comments_specifying_risks_en.pdf (europa.eu) (accessed on 16 February 2023).
[56] EDPS Formal Comments on the draft Commission Delegated Decision on further defining the risks related to security or illegal immigration or a high epidemic risk as defined in Regulation (EC) 767/2008, available at: 2022-0917_d2423_formal_comments_en.pdf (europa.eu).
[57] EDPS Formal Comments on the draft Commission Implementing Decision on specifying the risks related to security, illegal immigration or high epidemic risk as defined in Regulation (EC) 767/2008, available at: 22-06-29_formal-comments-illegal-immigration-or-epidemic-risk_en.pdf (europa.eu).
[58] C(2021) 4981 final, Recital 3.

as "distinguishable sets of observable qualities or properties based on information and statistics referred to in Article 33(2) of Regulation (EU) 2018/1240 and taking into account the data referred to in Article 33(4)(a) to (d) of that Regulation."[59] This essentially means that the sets of characteristics, which in the Commission's methodology need to be interpreted to identify specific risks, are derived from cross-checking statistics related to abnormal rates of overstaying, refusal of entry or of travel authorisations, and information provided by Member States (Article 33(2)) with data related to age range and sex; nationality, country and city of residence; and level of education and occupation (Article 33(4)). Based on the EDPS' Formal Comments to the (not publicly available) 'twin' delegated act on VIS, it appears that the exact same approach was adopted in that act as well.

This workflow raises a few concerns. First, one of the data sets used for establishing the 'sets of characteristics' includes data on nationality, and country and city of residence. Nationality and residence are dimensions that, if left unchecked, may determine patterns akin to differentiation based on ethnic aspects, because, depending on the third country at hand, they may be a sufficient ground for drawing assumptions as to the person's ethnic origin.[60] Secondly, the correlation of these data with data regarding age, sex, education and occupation might lead to yet more discriminatory profiles whereby groups of TCNs risk being categorised based on the relative weight of their current occupation or level of education, and their correlation with, for instance, their gender. In this regard, the most striking aspect is that the delegated act does not set out a methodology to determine the relative weight of all these dimensions (and of the statistical information referred to in Article 33(2)) in the definition of specific risks, nor does it establish sufficient safeguards against the risk that one or several of these dimensions get overrepresented in the definition of risks, and result, in turn, in unfair treatment vis-à-vis the specific groups of travellers who are attributed the resulting 'sets of characteristics'.

More generally, it does not appear that the ETIAS and VIS delegated acts fulfil (yet?) the mandate of Article 33(2) and 9j(2), respectively: instead of further defining the risks, as they shall under their legal base, the acts merely detail additional parameters for statistical analysis and appear to 'pass the hot potato' (i.e., *actually* define the risks) back to the ETIAS CU. This is particularly worrying because under the ETIAS and VIS Regulations the risk indicators, to be based on the further defined risks and the specific risks, will be established by the ETIAS CU, i.e., will be set unilaterally by an executive body outside the constraints and safeguards of the rules of procedures on law-making. That being so, it would be desirable to countervail this aspect by at least constraining the endeavour by the ETIAS CU via transparent risk assessment methodologies laid down in legal acts. However, if these legal acts (i.e., the delegated and implementing acts mentioned above) in practice entrust Frontex with defining the most critical aspects of the methodology, then individuals risk being deprived of the necessary transparency safeguards they are entitled to pursuant to the Court of Justice judgment *Ligue des droits humains* judgment.[61] Such rule-making practice is likely to make the whole system even more opaque

[59] *Ibid*., Article 2(b).

[60] With regard to the VIS delegated act, see EDPS, Formal Comments cited supra, note 56, para 15. In the same vein see also EDPS, Opinion 03/2017, cited *supra*, note 10, para. 40. Also, in the Case C-184/20, *OT v Vyriausioji tarnybinės etikos komisija*, the scope of sensitive data is interpreted broadly so that individuals benefit from the strengthened regime prescribed by the GDPR, by including data which have the potential of revealing sensitive information about the individual, despite not being inherently 'sensitive', as per Art. 9 GDPR. It means that factors such as nationality and demographic processed for automated risk assessment can be considered as sensitive data as long as the outputs are likely to reveal the ethnic origin of the TCNs. They might therefore be subject to the stringent processing conditions under the Art. 9 GDPR. See further CJEU, Judgment of the Court (Grand Chamber) of 1 August 2022 *OT v Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601, para. 125.

[61] C-817/19, para. 195. With regard to the pre-determined criteria mentioned in the PNR Directive, the Court observed that "[…] given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter […]".

than it would be if the algorithmic logic were to be built with a transparent approach: Burrell notes that "[w]hile datasets may be extremely large but possible to comprehend and code may be written with clarity, the interplay between the two in the mechanism of the algorithm is what yields the complexity […]".[62] However, if also the code – and the preliminary risk assessment methodologies and risk indicators – are obscure, the issue risks being amplified (see Section II below).

The above considerations may spark discussions on the extent to which the ETIAS and VIS screening rules risk infringing EU anti-discrimination law.[63] This is however not the main purpose of this paper: First and foremost, the above concerns tend to suggest that the process for defining specific risks, the resulting risk indicators, and the resulting screening rules for the algorithm might be opaque and insufficiently challenged by the various actors involved in the ETIAS and VIS decision-making activities. This points to an upstream, arguably more severe, flaw than the potentially discriminatory nature of the algorithm, i.e., a heightened difficulty reviewing the substance of algorithmic outcomes and thus in determining *whether* those outcomes show the symptoms of discrimination or other negative behaviour. This flaw is commonly referred to as 'opacity', which "stems from the mismatch between mathematical optimisation in high-dimensionality characteristic of machine learning and the demands of human-scale reasoning and styles of semantic interpretation."[64] As will become apparent in Section II of this paper, the less the algorithm rule-making process is opposable (via the letter of the law) and transparent, the more it runs the risk of negatively influencing the role of the authorities tasked with reviewing the algorithm's recommendations down the line. This is because meaningful human review of algorithmic outcomes could be jeopardised not only by scarce understanding of the variables used by the algorithms; but also, and perhaps more importantly, by the difficulty in interpreting how each variable contributed to the conclusion it generated.[65]

Are ETIAS and VIS automated processing examples of AI?

The automated characteristics of the ETIAS and VIS automated processing, in particular in relation to security, illegal immigration and high epidemic risks, trigger the question of whether the algorithm behind this processing qualifies as 'AI'. This question can be tackled from two main perspective: A software engineering perspective – that would entail discussing if the technical elements of the ETIAS screening rules fulfil the accepted definitions of AI in the data science realm; and a legal perspective – which becomes relevant especially in the light of the current AI Act proposal. For the purposes of our paper, we focus on the latter perspective and look at the definition of 'AI system' provided in Article 3(1) of the proposed Regulation, in the latest version amended by the Council in its General Approach of November 2022.[66] In that document, a system qualifies as 'AI system' if it "[…] is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts."[67]

---

[62] Burrell, J., *How the machine 'thinks': Understanding opacity in machine learning algorithms*, Big Data & Society, 3(1), 2016.
[63] See for instance Derave, C.; Genicot, N.; Hetmanska, N., cited *supra*, note 24.
[64] Burrell, J., cited *supra*, note 62., p. 2.
[65] Mittelstadt, B. D.; Allo, P.; Taddeo, M.; Wachter, S.; Floridi, L., *The ethics of algorithms: Mapping the debate*, Big Data & Society, 3(2), 2016.
[66] Council of the EU, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General approach, 25 November 2022, available at: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf.
[67] *Ibid*., Article 3(1).

How does the most recent definition relate to the ETIAS screening rules? As noted above, a full account of the algorithm that will support the ETIAS screening rules is currently not possible due to lack of information. However, valuable insights can be drawn from the reports of the European Commission and eu-LISA regarding the uptake of AI at Schengen borders.[68] In one of these reports,[69] after acknowledging that ETIAS applications triggering hits will be reviewed manually, states that "an additional level of automation or analytics based on AI or machine learning could be introduced when dealing with any 'suspicious' applications".[70] Such automation could take the form of a rule-based system for triaging, or of risk assessments that would require "more sophisticated system using one of the machine learning approaches (e.g. support vector machine algorithms […])."[71] By risk assessment, eu-LISA considers an approach whereby the algorithm would issue either binary recommendations for the authority to grant or refuse the travel authorisation or visa, or else more complex, non-binary recommendations based on various risk levels (we could imagine for instance a colour-coding system with different shades of green/yellow/red). Based on the ETIAS and VIS Regulations, which conceive the hit as the only possible output of the algorithm, it is clear that neither of these two explicit scenarios would be covered by the forthcoming ETIAS screening rules. However, what the ETIAS screening rules will do is trigger one binary outcome: based on the risk indicators used, they will either cause one or more hit to appear, or 'decide' not to trigger any hit. Even though this outcome would not amount to an explicit recommendation to reject or clear the application, it would still be an outcome based on the evaluation of certain parameters and criteria vis-à-vis the information included in the application. Compared to the risk assessment system envisaged by eu-LISA, the ETIAS logic might differ just because it lacks the 'next step': On top of the initial evaluation, which determines whether a hit is triggered (step 1), the ETIAS screening rules would not entail an *additional* evaluation, which would translate the set of hit/no-hit outcomes into an explicit recommendation for the human caseworker (step 2).

However, if step 2 existed, it would very likely be based on pre-determined parameters and thresholds allowing the system to formulate the 'approval' recommendation under – say – a given threshold of hits, or the 'rejection' recommendation above that threshold. But such a mechanism is essentially what the ETIAS screening rules will amount to – although their exact logic and parameters remain unclear; and therefore, if the risk assessment system (step 2) would qualify as AI, it follows that a system that follows a very similar logic – but only counts the first step – would be very likely to qualify as AI as well. Put differently, it is the system's underlying logic that should matter, not how many steps it applies that logic to. Such logic can, at the very least, be categorised as an example of 'rules-based' or 'knowledge-based' algorithm, which make decisions based on a set of pre-determined instructions and parameters.[72] It is noteworthy that under the definition of 'AI' currently upheld by the Council, whilst being more restrictive than the initial definition proposed by the Commission, knowledge-based algorithms still qualify as AI.

Having provisionally established, based on the available information, that the ETIAS screening rules are likely to qualify as rules- or knowledge-based AI, in the next section we show how the ETIAS screening

[68] Especially: eu-LISA, *Artificial Intelligence in the Operational Management of Large-scale IT Systems: Perspective for eu-LISA*, Research and Technology Monitoring Report, July 2020; European Commission, Directorate-General for Migration and Home Affairs, *Opportunities and challenges for the use of artificial intelligence in border control, migration and security. Volume 1, Main report*, Publications Office, 2020.

[69] eu-LISA, *Artificial Intelligence in the Operational Management of Large-scale IT Systems: Perspective for eu-LISA*, cited *supra*, note 68.

[70] *Ibid*., p. 30.

[71] *Ibid*.

[72] European Commission, Directorate-General for Justice and Consumers, Gerards, J., Xenidis, R., *Algorithmic discrimination in Europe: challenges and opportunities for gender equality and non-discrimination law*, Publications Office, 2021, p. 32.

rules might escape the *substantive* control of humans despite the safeguards *formally* provided in the law. We do so through the lens of EU data protection law mainly for two reasons.

Firstly, with the AI Act still being discussed by the EU co-legislators, data protection law contains the most relevant provision in force that a) aims to protect individuals directly, and b) captures the potential distortive effect of AI-driven practices, i.e., Article 22 GDPR / 24 EUDPR. Whilst designed to target a wider array of automation-based practices, these provisions can also contribute to building a 'legal firewall' against the spreading of AI-enabled mechanisms that, albeit constrained by a formally adequate oversight framework, are likely to *de facto* circumvent legal design. Secondly, based on its current text, the AI Act proposal would not be applicable to AI systems deployed within large scale information systems such as those established by the ETIAS and VIS Regulations, "unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned."[73] This provision has been met with sharp criticism by legal scholarship,[74] because it would allow AI systems such as the ETIAS screening rules to escape the prohibitions and safeguards of the AI Act. With this possibility on the horizon, Article 22 GDPR / 24 EUDPR becomes all the more important as the main secondary law provision capable of protecting individuals from the adverse effects of automated AI-based decision-making, should the *ex-ante* safeguards of the AI Act be rendered inapplicable. Via our analysis, we also purport that, in order for Article 22 GDPR / 24 EUDPR to be an effective protective tool, a 'dynamic' and purpose-driven reading these provisions should be preferred, steering away from a literal reading that might weaken their protection against fundamental rights violations (and which leads some authors to call for redrafting the provision to enhance its protective effect[75]).

Section II – The ETIAS and VIS Automated Processing and the Prohibition of Decisions Based Solely on Automated Means

The prohibition in Article 22 GDPR and Article 24 EUDPR

In this section, starting from the text of Article 22 GDPR and Article 24 EUDPR, we assess to what extent the ETIAS and VIS automated processing offer or are likely to offer the necessary safeguards for avoiding infringement of the prohibition of decisions based solely on automated means.

Article 22 GDPR reads: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[76] Such a decision, commonly but non unanimously seen as outright prohibited to data controllers,[77] can nonetheless be allowed (i) if it is necessary for entering into, or performing, a contract between the data subject and the controller; (ii) if it is authorised by EU or national law that also provides suitable safeguards for the data subject's rights and freedoms and legitimate interests; or (iii) if it is based on the data subject's explicit consent.[78] The provision of Article 24 EUDPR is essentially identical except for minor clerical differences.

---

[73] Article 83(1) of the AI Act proposal, left unchanged in the current General Approach by the Council.

[74] See for instance Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM), Statewatch, *Uses of AI in migration and border control: A fundamental rights approach to the Artificial Intelligence Act*, pp. 16 and seqq.

[75] See for instance De Hert, P.; Lazcoz Moratinos, G., cited *supra*, note 30.

[76] Article 22(1) GDPR.

[77] See for instance, arguing for the prohibition approach, Sancho, D., *Automated Decision-Making under Article 22 GDPR*, in Ebers, M.; Navas, S., Algorithms and Law, Cambridge University Press, 2020. For an opposite view, which qualifies the statement of Article 22(1) GDPR as a right to be exercised by the data subject, see, Tosoni, L., *The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation*, International Data Privacy Law, 2021, Vol. 11, No. 2.

[78] *Ibid*., paragraph 2.

The reading of the first two paragraphs of Articles 22 GDPR and 24 EUDPR implies, in essence, that two conditions must be fulfilled to argue that the ETIAS and VIS automated processing infringe EU data protection law: (i) first, it needs to be demonstrated that this processing leads to a 'decision' within the meaning of these articles; and (ii) if the first condition is verified, it needs to be demonstrated that the legal basis (i.e., the ETIAS and VIS Regulations) do not lay down sufficient safeguards for the data subjects. We analyse each condition separately.

Condition I – The result of ETIAS and VIS automated processing: A decision that significantly affects data subjects?

The prohibition of Article 22(1) GDPR and Article 24(1) EUDPR applies to *decisions* that are based *solely* on automated processing. Under a literal reading of this prohibition, only ETIAS would lead to a final automated outcome unchecked by humans, i.e., if the automated processing does not trigger any hits the system grants the travel authorisation automatically. However, this would be a *favourable* decision for the data subject; one that, according to the prevailing view in legal scholarship,[79] should not trigger the prohibition in line with the spirit of the provision, which targets *adverse* effects on individuals. In no other case does the processing lead to an unchecked outcome: in the ETIAS workflow a hit triggers the review by the ETIAS CU and, more thoroughly, by the ETIAS NU; in the VIS workflow, the competent visa authority reviews the application regardless of hits. Seemingly then, there would be no reason for concern: except for one scenario ('no-hits' response in ETIAS), human caseworkers are always going to check the application and confirm or dismiss the outcome of the automated processing.[80]

The issue with this conclusion is that the intervention of human reviewers, formally provided for by the law, may not be enough to rule out a decision with legal or similarly significant adverse effects on data subjects. In our assessment this may be due to two main reasons, which derive from two different interpretations of the term 'decision' in Article 22 GDPR / 24 EUDPR, i.e.: a) 'decision' as referring also to non-final outcomes of an automated processing; or b) 'decisions' as referring only to final outcomes. We explore both scenarios below.

Non-final automated outcomes qualifying as 'decisions'

One may argue that not only the final outcome of a given workflow can qualify as 'decision' for the purposes of Article 22 GDPR / 24 EUDPR, but that also the outcome of the automated processing, despite not being final, can qualify as such. This argument focuses not so much on the irreversibility of a given outcome, but on the causal link between that outcome and what follows down the line. Proponents of such argument purport that non-final outcomes generated by automated tools may qualify as 'decisions' if they condition upfront the later human decision-making window.[81] For instance, say that a VE-TCN applies for a travel authorisation and the ETIAS CS triggers two hits for security and illegal immigration risks, and after having examined the hits, the competent ETIAS NU decides to deny the travel authorisation. One might argue that the ETIAS CS-generated outcome (the hits) is in itself a decision because, without them being targeted by those two hits in the first place, the VE-TCN would not have been subject to a final decision by the ETIAS NU; in other words, that automated outcome would be the one taking the first step in determining the legal or similarly significant effects for the data subject.

We argue that this approach to interpreting Article 22 GDPR / 24 EUDPR should be discarded. This is because it risks overestimating the impact of an intermediary outcome in the automated processing

[79] See e.g., Veale, M.; Edwards, L., cited *supra*, note 26; 29WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2017.
[80] See for instance Derave, C.; Genicot, D.; Hetmanska, N., cited *supra*, note 24, p. 408.
[81] See for instance, although they do not purport the argument as such, Binns, R. and Veale, M., cited *supra*, note 42, pp. 325-326.

and underestimating the impact of the human-based outcome at the end. While it is true that, in the ETIAS/VIS scenario, the TCN's application would not be subject to human review *but for* the initial hit(s), the ETIAS NU still retains the power to grant the application. The same reasoning would apply under a system, akin to that envisaged at the end of Section I, whereby the ETIAS and VIS CS were to explicitly recommend that the human caseworker take a 'grant' or 'reject' decision, because the caseworker would still retain the ability to overturn that recommendation. Note here that the issue – at the core of this paper – of whether that human ability is meaningful is of course still relevant, but does not affect the endeavour of 'locating' the 'decision' in the workflow. If the review exerted by human caseworkers were to be merely formal and/or biased, then the possibility of construing the automated outcomes as 'decisions' for the purpose of Article 22 GDPR / 24 EUDPR would only be a consequence of the weakening of the *human* decision (located at the end of the process): Because the decisional autonomy of the human reviewer (that in principles qualifies his/her act as the decision) is reduced to a minimal degree, *then* the earlier automated outcome gains importance to the point that it may be regarded, in practice, as the decision itself. This is the focus of the next subsection.

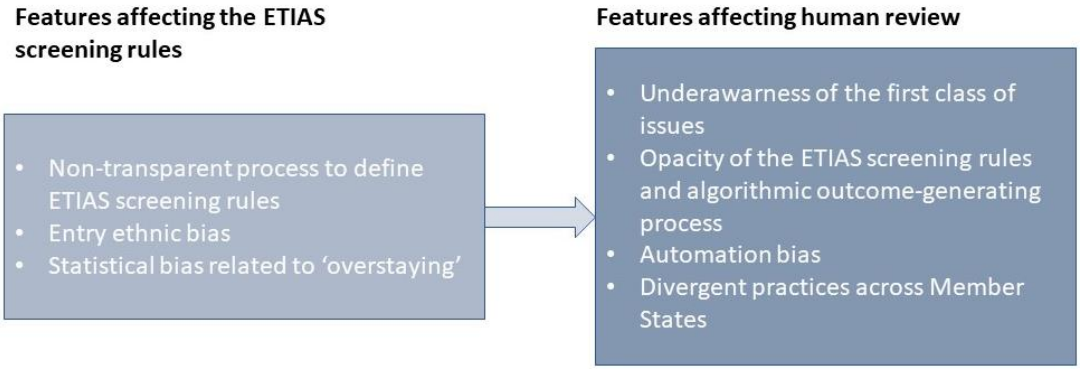
'Decisions' as only final outcomes

We argue that, as long as a non-final outcome of an automated processing still leaves the door open to a different recommendation, it does *not* qualify as 'decision'; then the risk of running afoul of Article 22 GDPR / 24 EUDPR would depend on the relative weight of the outcome of the automated processing and the human review. We can distinguish two sub-scenario: In the first sub-scenario, the problem may reside in the formalistic and non-substantial nature of the human review at hand. Being well aware of such possibility, the 29WP writes in the Guidelines on Article 22 that "The controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture."[82] Of course, it is not easy to ascertain *in abstracto* whether human intervention is merely formalistic; while the law may give crucial indications as to whether this is the case (e.g., based on the list of powers that the law entrusts the reviewers with), the practice on the ground is also necessary to a comprehensive assessment. In the second sub-scenario, we can imagine that the human intervention is initially anything but formalistic or non-substantial, but its real weight gets thwarted in the long run by a subtle form of the so-called 'automation bias'. In practice, automation bias occurs when humans get unduly influenced in their decision-making by the authoritative outcome-generation of an automated system, such as an AI system.

We submit that several features of the ETIAS and VIS automated processing may induce human reviewers to *think* they keep applying the same level of scrutiny over the automated outcome, while the influence they have on the final decision actually decreases and becomes little or no more than rubber-stamping. In other words, because of its design, the ETIAS and VIS automated processing is likely to give rise to a risk of non-meaningful human review that may be reinforced by automation bias going forward, thereby possibly creating outcomes that would qualify as decisions based solely on automated means.[83] The figure below collects the features that, combined, may cause these effects. As can be seen from the figure, we distinguish between features depending on when they occur in the overall workflow: a) features that occur when the automated process is running; and b) features that are inherent to the ETIAS screening rules but that prevent or limit the human caseworkers' ability to meaningfully review and, if necessary, challenge the automated outcome *ex-post*, during the manual review.

[82] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 21, available at: https://ec.europa.eu/newsroom/article29/items/612053.
[83] See also Zandstra, T.; Brouwer, E., cited *supra*, note 10, p. 3.

Figure 4: Features of the ETIAS screening rules that may lead to decisions based solely on automated means



Features affecting the ETIAS and VIS automated processing

The first category of features, i.e., those that intervene while the ETIAS and VIS automated processing is running, are both examples of *bias*. Before delving into them, it is worth noting that algorithms make biased outputs (recommendations, decisions, etc.) by default, by their very nature.[84] This is because any algorithm, including the ETIAS/VIS algorithm, originates from a design and configuration established by humans, whose priorities, values and humans-generated constraints (e.g., regulatory requirements) inevitably shape the algorithm's rules and functioning logic at the outset. These priorities, values and constraints determine a design choice that is precisely a *choice* amongst other possibilities.[85] In this respect, any algorithmic outcome is biased vis-à-vis an ideal set of perfectly objective and neutral criteria. For instance, the decision to use in the ETIAS screening rules the job group entry in combination with the education level, instead of just either of them, is going to carry an inherent bias, irrespective of potentially discriminatory outcomes of such design choice. Because of this inherent 'existential' bias of algorithms, it is important to prevent *additional* biases from degrading their outcomes. However, we show how two more biases are likely to affect the ETIAS/VIS algorithm.

'Ethnic entry bias'

We refer to 'ethnic entry bias' to refer to a distorted approach to applying the legally stipulated conditions for allowing or refusing TCNs entry into the Schengen area. A study by FRA[86] has showed that Schengen border authorities are not immune from applying 'ethnic lenses' when identifying travellers who may be attempting to cross the external borders illegally. This finding is relevant to our discussion insofar as, pursuant to Article 33(2)(c) of the ETIAS Regulation, the "information substantiated by factual and evidence-based elements provided by Member States concerning abnormal rates of […] refusals of entry for a specific group of travellers […]"[87] is amongst the informational sources the Commission shall use to define the security, illegal immigration and high epidemic risks. To the extent that this information by Member States integrates refusal of entry statistics that are affected by an ethnically non-neutral approach to border checks, this bias is likely to be incorporated into the risks and, in turn, into the risk indicators for the ETIAS screening rules.

This *vulnus* would, depending on its extent, trigger interesting discussions from a non-discrimination point of view; but it would also be a hidden distortion that the algorithm 'ingests' and lives by, making it very difficult for the competent authorities to detect it and correct it. So again, it may be the basis

[84] Mittelstadt et al., cited *supra*, note 65, p. 7.
[85] *Ibid*.: "An algorithm's design and functionality reflects the values of its designer and intended uses, if only to the extent that a particular design is preferred as the best or most efficient option."
[86] European Union Agency for Fundamental Rights, *Fundamental Rights at Airports: Border Checks at Five International Airports in the European Union* (2014) 45.
[87] Article 33(2)(c) ETIAS Regulation.

not *just* for discriminatory automated recommendations, but for discriminatory automated recommendations that human reviewers would be underequipped to scrutinise.

Statistical bias

Statistical bias is another type of bias that may be carried over by the algorithm of the ETIAS screening rules. It also links back to Article 33(2)(c) ETIAS Regulation, which requires Member States to provide information and elements concerning abnormal rates of overstaying. While overstaying appears to be a *prima facie* valid proxy to judge illegal immigration risk, statistics related to overstaying may be distorted by the fact that asylum applicants whose application is pending are in all likelihood going to be counted in as 'overstayers'. This is because Article 2(3) of Regulation 2226/2017 ('EES Regulation'), which specifies the categories of persons to which the EES Regulation, and thus the concept of 'overstaying', does not apply, does not include asylum applicants waiting for a decision on their application.[88] Until they receive a decision, then, although they are authorised to stay in the Schengen area, they are likely to be registered as overstayers and thus populate the database ingested by the ETIAS screening rules for the purpose of identifying illegal immigration risk. As a result, the 'overstayers' category of the statistics used by the ETIAS/VIS algorithm is likely to get inflated by asylum applicants, and thus a) get bigger than if only data about illegal overstayers were collected; and b) be affected by the particular sets of characteristics of asylum applicants. The ultimate outcome of this bias may be to unduly distort the actual sets of characteristics considered by the ETIAS/VIS algorithm, which then risks targeting (via hits) different groups of people than it would if asylum applicants were left out.

This possible bias in the ETIAS screening rules is an example of a larger issue that concerns the reliability of algorithmic outcomes based on statistics and categorisation. It has been observed in scholarship that statistical methods, while they can build correlations between inputs, do not necessarily highlight causal connections between them and may not provide sufficiently conclusive evidence for decision-making.[89] The above statistical bias may lead to discriminatory outcomes, but even before that, may contribute to rendering human oversight meaningless in the long term. The example of an AI-based law enforcement tool deployed in a British police force, the Harm Assessment Risk Tool ('HART'),[90] is illustrative. Scholars observed that, absent ad-hoc safeguards, the tool might create vicious cycles of bias. Let us say that the algorithm is designed to label as 'high-risk' based on the weight of certain variables. If these variables are mostly found in certain circumscribed areas, then "more people from these areas will come to police attention and be arrested than those living in lower-risk untargeted neighbourhoods. These arrests then become outcomes that are used to generate later iterations of the same model, leading to an ever-deepening cycle of increased police attention."[91] The ETIAS screening rules might lead to such feedback loops, except that, under the expected configuration of these rules, feedback loops would be reflected in a higher number of hits rather than in a formal 'high-risk' label or similar.

---

[88] Article 2(3) EES Regulation does exclude from its scope of application "holders of residence permits" listed in Article 2(16) of Regulation 2016/399 ('Schengen Borders Code'); but the Schengen Borders Code states that such residence permits include "[…] all other documents issued by a Member State to third-country nationals authorising a stay on its territory […] *with the exception of:* […] *an application for asylum*" (emphasis added). Asylum applications are therefore not amongst the permits the holders of which fall outside the EES provisions on overstaying. See also Derave, C., et al., cited *supra*, note 24, pp. 413-414.

[89] Mittelstadt, B. D. et al., cited *supra*, note 65.

[90] Developed for the Durham Constabulary in cooperation with Cambridge University. See: https://www.cam.ac.uk/research/features/helping-police-make-custody-decisions-using-artificial-intelligence.

[91] Oswald, M.; Grace, J.; Urwin, S.; Barnes, G. C., *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality*, Information & Communication Technology Law, 2018, Vol. 27, No. 2, p. 228.

The key problem with this outcome for our purposes is that the more the bias reinforces via the ever-continuing feedback loops, the less visible it becomes, to the point where human reviewers risk losing the ability to retrace the bias to its origin. In such a scenario, human reviewers would end up 'buying in' the bias in their manual review, with no real awareness of and/or ability to correct the overall decision-making process. In the ETIAS example, the risk is that the inclusion of asylum applicants in overstaying statistics for the purpose of illegal immigration risk over time leads to an ever-depending cycle: The more sets of characteristics shared *inter alia* by asylum applicants are visible to the algorithm, the more the algorithm is likely to 'sanction', with hits, those ETIAS and VIS applicants that share those characteristics. Now, of course the application would then be reviewed by the competent authorities; however, especially if the opacity and automation bias tendencies (see below) self-reinforce, the reviewing authorities run the risk of relying excessively upon the constant and ever-confirmative flow of hits triggered on the same sets of characteristics as a warning sign of illegal immigration risk, and risk being unable to detect whether a particular applicant was actually caught because of his/her situation as asylum applicant.

Features directly affecting human review

The above factors may be enough to criticise the foundations of the ETIAS and VIS automated processing from a non-discrimination law perspective. Scholars have indeed focused on these features to show that the ETIAS screening rules are likely to generate discriminatory outcomes, including proxy discrimination.[92] At the heart of this issue is the idea that the ETIAS and VIS profiling is going to single out, and subsequently examine, individuals based on shared sets of characteristics more than on their personal situation and/or behaviour.[93] Our intent, however, is to show that the ETIAS screening rules, and the automated processing associated with it, are likely to reduce human influence over their outcomes, including the ability to detect and challenge such potentially discriminatory effects. This is why we also address the following features.

Under-awareness of the first category of features

The first risk related to the non-automated part of the decision-making process is that human reviewers (i.e., visa authorities and ETIAS NUs) are not or insufficiently aware of the above-mentioned features. The less someone is aware of a flaw in a mechanism, the less likely they are to look for it and to come up with strategies to mitigate it. This problem may well be amplified by a lack of understanding and training. In the context of a fairly advanced AI policing tool, it was noted that with over 4.2 million interdependent decision points, for non-specialists to understand and actively challenge the decision-making logic of the model may be a dauting task.[94] While the algorithm behind the ETIAS screening rules is likely to be simpler, a knowledge gap between the algorithm and the reviewers supposed to monitor its outcomes is also quite likely. This problem has been addressed in the literature as a special category of opacity, namely 'opacity as technical illiteracy'.[95]

Opacity of the ETIAS screening rules and of the algorithm

[92] Derave, C. et al., cited *supra*, note 24., p. 415-417. See also FRA, Opinion 02/2017, cited *supra*, note 15, p. 29; FRA, *Getting the future right: Artificial intelligence and fundamental rights*, 2020, p. 11, available at https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights.

[93] Vavoula, N., cited *supra*, note 21., p. 464-465: "[TCNs] will be flagged not because of any specific actions they have engaged in but because they display particular category traits in a probabilistic logic devoid of concrete evidence." The core of this problem is to what extent a risk-based approach typical of traditional migratory policies – that will inevitably rely at least *partially* on shared traits as evidence, and not wholly on individual characteristics – is compatible with EU fundamental rights law applicable to TCNs seeking to enter the Schengen area.

[94] Oswald et al., cited *supra*, note 91., p. 234.

[95] Burrell, J., cited *supra*, note 62, p. 4.

Possibly the most crucial feature of the ETIAS and VIS automated processing is the opacity behind the granular foundations of its rules – risk indicators and screening rules, already pointed out in Section I. When discussing the proportionality of automated rules-based mechanisms in its *PNR* Opinion,[96] the CJEU developed, amongst others, two key guidelines: a) that "the pre-established models and criteria [of the algorithm] should be specific and reliable, making it possible […] to arrive at results targeting individuals who might be" reasonably linked to the policy objective at hand (i.e., suspicion of participation in terrorist or serious transnational crime in the PNR case; security, illegal immigration, or high epidemic risk in the ETIAS and VIS case);[97] and b) "[…] any positive result obtained following the automated processing of [passenger] data must […] be subject to an individual re-examination by non-automated means before an individual measure […] is adopted."[98] If we focus on each guideline in isolation, as of now it is hard to say whether the ETIAS screening rules satisfy the former guideline: Depending on how the risk indicators and the screening rules themselves are designed to work, they may or may not be granular enough to deploy a targeting scheme that is based on a 'reasonable' link between the individual and the risks considered. For the time being, however, the fact that the ETIAS screening rules will be heavily based on 'sets of characteristics' in turn grounded on data points such as nationality, residence, and job group, makes it likely that the algorithm will be driven more by categorisation than by the specificities of individual situations that a few data points can by no means thoroughly comprehend.[99] Conversely, on paper, one might say that the ETIAS and VIS automated processing satisfies the latter guideline, as human review of hits is mandatory by law. What is more, the ETIAS and VIS Regulations prescribe that the competent authorities shall never "take a decision automatically on the basis of a hit based on specific risk indicators. The [competent authority] shall *individually* assess the security, illegal immigration and high epidemic risks in all cases" (emphasis added).[100]

However, it is also worth reading the two guidelines established by the Court *in conjunction*. For the guideline requiring human re-examination to be meaningful and actionable, it needs to be applied to a situation whereby the guideline requiring 'specific and reliable' criteria is also complied with. The idea is that the human reviewer is able to 'reverse-engineer' the automated outcome, understand why the algorithm reached a given result, and verify if the overall evidence confirms it or dismisses it. However, this goal is likely to not be met a) if the logic underpinning the rules-based model is not sufficiently specific and reliable, especially if the algorithm is designed to trigger hits based on associating natural persons with pre-established categories; and b) if reviewers do not have a thorough view of the relative weight of all the factors taken into account by the algorithm. Because of the first flaw, the criteria that triggered the hit(s) may be too generally applicable for reviewers to thoroughly verify if they were applied justifiably or not to a *specific* individual situation. And because of the second flaw, human reviewers are likely to be less equipped to unpack the automated outcome-generating process and reconstruct the causal links between the specific situation of a TCN and the presence of one or more hits. We echo on this point the EDPS, which, "given the lack of transparency in the process of creating profiles", expressed strong doubts as to the ability of the ETIAS CU and NUs to "[guarantee] a real in-depth scrutiny of the detected potential risks" and "assess the hit based on the ETIAS screening rules on its merits."[101]

[96] Court of Justice of the EU, Opinion of the Court (Grand Chamber) of 26 July 2017.
[97] *Ibid*., para. 172.
[98] *Ibid*., para. 173.
[99] Derave, C.; Genicot, N.; Hetmanska, N., cited *supra*, note 24.
[100] Article 20(5) ETIAS Regulation; Article 9c(6) VIS Regulation.
[101] EDPS, Opinion 3/2017, cited *supra*, note 10, para. 37, p. 11.

These flaws may also lead to a lack of comparability across outcomes: For instance, three different citizens of the same third country may be all subject to a hit for illegal immigration risk; this may be the result of different combinations of baseline data – same nationality, but potentially different education level and job group: If human reviewers do not know what relative weight does the algorithm assign to each data point in correlation with all other data points, then they are unlikely to understand what features of each person's individual situation played a decisive role in triggering the hit(s); in turn, they are then unlikely to apply a meaningful review, that is, verify if the algorithm was justified in its assessment, and evaluate any countervailing evidence, including if there are (and which ones) any discriminating factors that may overturn the automated outcome.

Because of the non-transparent approach to establishing the risk indicators and the screening rules, and because of its reliance on (potentially discriminatory) very generic sets of characteristics, the ETIAS and VIS automated processing is likely to be affected by the mutually reinforcing effect of the above-mentioned flaws. It is worth noting that these two flaws correspond by and large to two of the key ethical issues raised by algorithms, i.e., as Mittelstadt et al. put it, 'inscrutable evidence leading to opacity' and 'misguided evidence leading to bias'.[102] As such, we submit that the ETIAS algorithm would be unlikely to satisfy the two guidelines established by the Court in *PNR* and confirmed in later case law. It is not enough to draft a regulation that requires authorities to manually review automated recommendations. The whole system shall be designed with a 'human in the loop' by design approach, i.e., so as human reviewers do not merely get to approve or reject the algorithmic outcome, but are also enabled to thoroughly dissect it.

At this point, it is easy to get tangled up with the question as to what extent the human review of the outcome generated by an AI system, with an incomparably grater processing power than the reviewers themselves, needs to be comprehensive to be deemed legally appropriate. Are humans really expected to thoroughly understand how an AI system 'thinks'? Can they do so on a regular basis, for thousands, millions of individual applications? These are questions that arise in all socially relevant contexts where AI is deployed.[103] The answers may depend on the complexity of the AI system we are dealing with.[104] But at the outset, we observe that a policy and regulatory approach to AI that were to revolve around these answers, would run the risk of surrendering the values of a democratic human-centric society in case of a negative answer – or at least, an answer that is different from "yes, in all circumstances." *Unless* meaningful scrutiny of AI-based recommendations is ensured – and what 'meaningful' means is of course up for debate – AI cannot be deployed in compliance with the framework of fundamental rights and values that we want our lives to be governed by. In other words, if we still want AI to be used under the constraints of these values and rights, specifically for the societal and individuals' own good, human control *must* ultimately be guaranteed.[105] This is especially crucial because AI-based outcomes do not come with their inherent meaning: They are mathematical elaborations whose meaning is ultimately attributed by humans;[106] but if the human filter is devoid of substance, we run

[102] Mittelstadt, B. D. et al., cited *supra*, note 65, p. 4.

[103] Burrell, J., cited *supra*, note 62.

[104] *Ibid*., p. 9: "With greater computational resources, and many terabytes of data to mine (now often collected opportunistically from the digital traces of users' activities), the number of possible features to include in a classifier rapidly grows way beyond what can be easily grasped by a reasoning human".

[105] See Oswald, M. et al, cited *supra*, note 91, p. 235: "Our view is that the argument that 'it's a black box and therefore inscrutable' can no longer hold valid in relation to public sector use of algorithms, if it ever was."

[106] More generally, no information does 'necessarily imply the attribution of meaning, as it may in the case of humans', see Hildebrandt, M., *Law As Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics*, 2017, p. 10, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2983045; see also Silver, N., who argues that "the numbers have no way of speaking for themselves. We speak for them. We imbue them with meaning' which might be 'self-serving", Silver, N., *The Signal and the Noise: The Art and Science of Prediction*, Penguin, 2013.

the risk of letting automated outcomes self-attribute an unchallenged meaning in the form of a clearly actionable consequence for individuals.

Automation bias and informal 'rulebooks'

Opacity is an 'original sin' of algorithmic systems that inhibits meaningful scrutiny even when human reviewers are conscious and willing to perform it. It is an objective limitation to fulfilling the duty to challenge automated recommendations. The impact of opacity on decision-makers' ability to prevent decisions based solely on automated means can however be reinforced by another factor: automation bias. Historically, automation bias has been conceived as the result of 'commission errors' – whereby human reviewers follow the automated recommendations and neglect countervailing evidence at their disposal; or 'omission errors' – whereby human reviewers ignore or are not informed of problems affecting the automated system and its ability to generate outcomes as expected.[107] Hence, this type of bias affects the human review process in practice, rather than to the algorithm per se. Oswald et al., discussing the UK-deployed HART system, warn against underestimating such issue. They conceive the possibility that the algorithmic support ultimately leads certain human reviewers (custody officers in that case) to a state of 'judgmental atrophy',[108] whereby, that is, humans tend to make more and more often the algorithmic recommendation their own. Specifically, the authors point out that "we must not only consider the code […] but also the way that it might 'mesh' into a police force, its routines, objectives and decision-making processes."[109]

As the law stands, no specific mechanisms are envisaged to protect ETIAS NUs and visa designated authorities from automation bias. The high amount of data and information that will be cross-checked by the ETIAS and VIS CSs as part of the automated processing of applications is likely to aggravate this risk. This is because, the more databases are queried, and the more data-to-data correspondences are checked in those databases, the higher the likelihood that applications will be subject to hits. There is therefore the possibility of high flows of applications flagged by a number of hits not just against the security, illegal immigration, and high epidemic risks, but also against the other data points mentioned in Article 20 ETIAS Regulation and Article 9a VIS Regulation.

This can lead to two challenges: First, and fundamentally, a challenge related to the 'authority' of the automated outcomes produced by the ETIAS screening rules. Let us consider a scenario whereby the ETIAS screening rules tend, over a certain period of time, to consistently trigger security risk hits on multiple applications that share common sets of characteristics, for instance 'set 1'; in the first months of operations, the caseworkers within the competent authorities may thoroughly review the automated outcomes (whilst being subject to the opacity and biases mentioned above) and, for instance, conclude that most of those applications do in fact pose a security risk and reject them. The risk with these dynamics is that the caseworkers unwittingly associate the *consistent* flagging of 'set 1' by the algorithm with the conclusion reached *in most cases* after human examination. In other words, there is a risk of taking the initial statistical correspondence between automated and human outcomes as 'proof' that the set of characteristics 'set 1' is indicative of security risk. As a result, human examination might become less and less intense and thorough over time over 'set 1' applications, thereby increasingly taking the algorithmic outcomes as sufficient evidence to grant or reject. The more the algorithm exerts its authority also on other sets of characteristics ('set 2', 'set 3', etc.), the higher the share of automated outcomes that risk being subject to a weaker degree of genuinely

[107] See for instance Skitka, L. J.; Mosier, K. L.; Burdick, M.; *Does automation bias decision-making?*, International Journal of Human-Computer Studies (1999) 51, p. 993.
[108] Oswald et al., cited *supra*, note 91, p. 232.
[109] *Ibid*., p. 225. See in this respect Beer, D., *The social power of algorithms*, Information, Communication & Society 2017, Vol. 20, No. 1, pp. 10-11.

human review. The result may be the creation of 'informal rulebooks', i.e., unofficial decision-making mechanics that are reiterated by the human caseworkers based on the past authoritative influence of the algorithm. Other hits against databases may also have a reinforcing effect on the algorithmic authority related to security, illegal immigration, and high epidemic risk: Let us consider an application flagged for security risk, over which the competent authority may already suffer from automation bias by the ETIAS screening rules; if the application is also subject to hits against, say, an alert in SIS or a data record in ECRIS-TCN, then the amount of automatedly generated information pointing towards a security risk is even higher. In other words, the amount of presumptive (but in principle and legally non-conclusive) evidence would increase starting from a situation whereby the authority is already potentially subject to automation bias for a particular set of characteristics.

Second, we submit there is also a *time-related challenge*. In principle, each hits needs to be verified in-depth to make sure that legal consequences only flow from them after the competent authority has verified the context and situation that triggered that hit. Each manual verification process may take time and effort, and may require, as also envisaged by the legislation, consultations with authorities of other Member States who either were responsible for inputting the data points or have useful information to review the hit.[110] Against this backdrop, doubts can be raised as to whether human caseworkers will in the long run be able to devote a sufficient amount of time to each hit related to security, illegal immigration, and high epidemic risk, so as to ensure their decision-making independence vis-à-vis the outcomes of the ETIAS screening rules. It is worth noting in this respect that the ETIAS NUs will have to take a decision on each admissible application within 96 hours from its lodging.[111]

Divergent practices at Member State level

Finally, the opacity of the ETIAS screening rules and the automation bias may lead to a third 'knock-on' effect. As is well-known, Member States' legal migration policies are only partially harmonised at EU level, and are still subject to national priorities and objectives. These translate, for instance, into the national visa policies that still exist aside the Schengen visa policy. One possible undesired effect of the ETIAS screening rules is that the objectives of the various national migration policies creep into the manual review of VIS and ETIAS hits as a result of the lack of predictability of the review methodology. The harder it is – as we observed above – for human reviewers to reconstruct the chain of events that led the algorithm to a result, the higher the chance that the automated process leaves a shred of uncertainty as to how to interpret its outcomes. Therefore, lacking a scientifically predictable process that guarantees an objective reading of all hits, the interpretation that ETIAS NUs and visa authorities will give might not be wholly harmonised across Member States, especially in complex cases with multiple hits; it might also be somewhat affected by national migration policy priorities.

Takeaways related to condition I

The section above analysed the reasons why the ETIAS and VIS automated processing might set the ground for algorithmic outcomes capable of qualifying as decisions based solely on automated means, whereas the 'solely' concept stems from an insufficiently equipped or thorough human review. Another set of reasons relates to the way the ETIAS screening rules are likely to be conceived and developed, and to the bias they are likely to carry. Another set of reasons concerns the activity of human caseworkers being confronted with the automated outcomes, and likely to be subject to opacity, automation bias, and divergent practices across Member States.

[110] For instance, Articles 26(3), 28 ETIAS Regulation.
[111] Articles 30 and 32 ETIAS Regulation.

This potentially decreasing control by humans over outcomes generated by the ETIAS screening rules can could also be reinforced by other challenges, particularly by developments of the algorithm itself. While the above challenges can already be produced by the set of parameters and rules pre-established by developers, what would happen if the algorithm started building 'its own' decision-making routine based on the experience it develops?[112] It may be that the algorithm supporting the ETIAS screening rules does not, as such, possess machine-learning or other learning capabilities. However, the Commission and eu-LISA have reported to envisage an increasing role for AI in the border control and migration contexts.[113] To the extent that the ETIAS and VIS algorithm are planned to be upgraded in the future, the above risks should be taken into account by default in order to focus on the risks of more elaborate and sophisticated algorithmic decision-making capabilities, which can create new rules on top of the pre-defined ones, and have the potential to be even more opaque. The impact of sophisticated AI technologies on opacity, and especially in scenarios where opacity is already an issue, is crucial, because "[w]hen a computer learns and consequently builds its own representation of a classification decision, it does so without regard for human comprehension."[114]

Condition II – Safeguards for data subjects

Provided that condition I is met, Article 22 GDPR and Article 24 EUDPR would necessitate adequate safeguards for TCNs rights and freedoms to allow ETIAS and VIS automated processing. The need for adequate safeguards becomes especially pertinent considering that such processing might infringe on a number of fundamental rights, such as the right to private and family life,[115] the right to personal data protection,[116] the right to an effective remedy and to a fair trial.[117] One of the prominent safeguard against the undesired impacts of the fully automated decisions is human intervention, which should be complemented by additional measures to the benefit of data subject rights.

'Properly functioning' human intervention

As highlighted by the CJEU in Opinion 1/15[118] and reiterated in *Ligue des droits humains* judgment,[119] human intervention must be considered as a minimum safeguard for decisions made solely by automated means. It means that the appropriateness of the ETIAS and VIS screening rules depends on the 'proper functioning' of the human intervention on non-automated means. As highlighted in the *PNR* case, it serves to minimise "the number of innocent people wrongly identified" by a system which may produce a "fairly substantial number of 'false positives'".[120] Also, the envisaged human intervention should exclude any discriminatory results from the automated processing. Similarly, Article 14 ETIAS Regulation and Article 7 VIS Regulation prohibit discrimination against TCNs on protected grounds.

Human involvement in the ETIAS and VIS processing

Article 22 ETIAS Regulation requires the involvement of human agents from the ETIAS CU to check the genuineness of the hits. However, this does not necessarily provides sufficient safeguards because the

[112] See Gal, M. S., *Algorithmic Challenges to Autonomous Choice*, Michigan Technology Law Review, 2018, Vol. 25, Issue 1, p. 6.
[113] eu-LISA, *Artificial Intelligence in the Operational Management of Large-scale IT Systems: Perspective for eu-LISA*, cited *supra*, note 68.
[114] Burrell, J., cited *supra*, note 62, p. 10.
[115] Article 7 of the EU Charter of Fundamental Rights.
[116] Ibid., Article 8.
[117] Ibid., Article 47. See also 29WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 27.
[118] C-817/19, *Ligue des droits humains v Conseil des ministres*, judgment of 21 June 2022, ECLI:EU:C:2022:491.
[119] *Ibid*., para. 203.
[120] *Ibid*., para. 123.

ETIAS CU merely 'verifies' formal features of the processing and transfers the hit to ETIAS NU.[121] Once a hit is reported to the competent ETIAS NU, Article 26(6) ETIAS Regulation obliges it to *"individually* assess the security, illegal immigration and high epidemic risks in all cases". In this regard, in no circumstances may the responsible ETIAS NU of the Member State take a decision automatically on the basis of a hit based on specific risk indicators. The same human intervention mechanism for ETIAS NU is also envisaged and applies to immigration authorities in the context of VIS.[122] However, as explored in Section II, the envisaged human intervention mechanism may not function properly on several grounds, including the opacity of the pre-determined criteria and automation bias.[123]

Pursuant to Article 8(3) ETIAS and, Member States are obliged to provide the ETIAS NUs with adequate resources to fulfil their tasks in accordance with the deadlines set out in this Regulation. This provision should enable ETIAS NUs to provide necessary training to human agents for meaningful human intervention. Otherwise, the human intervention safeguard may not be as meaningful as envisaged. An example of best practice for human intervention in this context is the 'four eyes principle'. It essentially means that the ETIAS NU or immigration authority would take a decision only after at least two agents within the authority have been consulted and have jointly agreed to a given course of action.[124] This principle might be integrated in the various Handbooks prepared by the European Commission *inter alia* for border authorities.

Data Subject Rights

If the data processing operations carried out under ETIAS and VIS fall under the automated processing described under Article 22(1) and (4) GDPR, it must be accompanied by adequate safeguards for the data subjects. Other than general notices online, TCNs will be notified with the necessary information about their rights[125] and how to exercise them as stated under Article 38 of the ETIAS and VIS Regulations. Furthermore, certain rights are particularly important to contest the decision and hence to enable individuals to enjoy their right to effective judicial remedy. As stipulated under Articles 13, 14 and 15 GDPR, the TCNs must be provided with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the concerning TCNs.[126]

In compliance with the transparency principle, also the decision-making procedure needs to be clearly communicated to the TCNs. Considering that even agents involved in the decision-making might have challenges with regard to understanding the screening rules and logic behind the automated processing(see Section II above), the right to comprehensive and thorough information becomes crucial. This issue is relevant in relation to the CJEU's statement that the use of certain machine learning technologies 'would be liable to render redundant the individual review of positive matches and monitoring of lawfulness", since the opacity of the technology might make it "impossible to

[121] Article 22(4) ETIAS Regulation mandates the deletion of false positives. Under Article 7(4) ETIAS Regulation, the periodic reports concerning false hits shall be provided by the ETIAS CU to the Commission. Until then, there will be limited information on the accuracy and trustfulness of the automated systems in use.

[122] Article 9 VIS Regulation.

[123] Eklund, A. M., cited *supra*, note 25.

[124] See, also for the advanced human intervention mechanism developed by the Netherlands Police. World Economic Forum, *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations (Revised 2022)*,pp. 11-12, available at https://www.weforum.org/reports/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case-law-enforcement-investigations-revised-2022.

[125] In particular, the information on the procedures for exercising the rights under Articles 13 to 16 of Regulation (EC) No 45/2001 and Articles 15 to 18 of Regulation (EU) 2016/679

[126] Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR. Please note that in the law enforcement context the exercise of data subject right is differs. See, Quintel, T., cited supra, note 23.

understand the reason why a given program arrived at a positive match".[127] According to the Court, this could deprive the data subjects of their right to an effective judicial remedy enshrined in Article 47 of the EU Charter of Fundamental Rights, a right which requires a high level of protection "in particular in order to challenge the non-discriminatory nature of the results obtained".[128] This is also highlighted in the CJEU *R.N.N.S.* judgement, concerning the refusal of a visa, the person concerned must be able "to ascertain the reasons upon which the decision taken in relation to him or her is based, either by reading the decision itself or by requesting and obtaining notification of those reasons".[129]

Other safeguards

Article 10 ETIAS Regulation establishes an independent ETIAS Fundamental Rights Guidance Board[130] which will perform regular appraisals and issue recommendations on the application of screening rules and its implications on fundamental rights, particularly regarding privacy, personal data protection and non-discrimination. Although the decisions or recommendations by the Board are not binding, it will serve as an additional guarantee against possible shortcomings arising from the system in practice. Also, the Board will produce publicly available annual reports that may contribute to transparency and reduce the informational asymmetry of data subjects.

The national Data Protection Authorities ('DPAs') will monitor the application of the data protection rules, including the effective exercise of data subject rights of TCNs in the context of ETIAS and VIS automated processing in their respective countries. Also, the EDPS will supervise the ETIAS and VIS automated processing in the central system managed by eu-LISA and the ETIAS CU managed by Frontex. In accordance with the data protection principles, all TCNs whose data is processed in the context of ETIAS and VIS automated processing are accorded specific rights.[131] These rights are a) right to access data relating to them stored under ETIAS and VIS; b) the right to correction of inaccurate data or deletion when data have been unlawfully stored; and c) the right to bring proceedings before the courts or competent authorities to correct or delete data or to obtain compensation.

Takeaways related to condition II

As also noted by European Digital Rights ('EDRi'), the AI-based risk assessments in the migration context are inherently opaque and difficult to contest due to the power imbalance. Affected TCNs have no means to access the risk parameters used in these assessments or challenge them effectively if they result in discriminatory or inaccurate outcomes.[132] Overall, this could lead to significant and harmful decisions such as detention and deportation, which could have a profound impact on TCNs. While

[127] C-817/19, para. 195.

[128] *Ibid*., para. 195.

[129] Joined Cases C-225/19 and C-226/19 R.N.N.S. and K.A. v Minister van Buitenlandse Zaken, judgment of 24 November 2020, ECLI:EU:C:2020:951, para. 43.

[130] Article 10 ETIAS Regulation is included following the study for the LIBE committee, Alegre et al. *European Travel Information And Authorisation System (ETIAS): Border Management, Fundamental Rights And Data Protection*, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583148/IPOL_STU(2017)583148_EN.pdf. The board "composed of the Fundamental Rights Officer of the European Border and Coast Guard Agency, a representative of the consultative forum on fundamental rights of the European Border and Coast Guard Agency, a representative of the European Data Protection Supervisor, a representative of the European Data Protection Board established by Regulation (EU) 2016/679 and a representative of the European Union Agency for Fundamental Rights."

[131] Article 38 ETIAS Regulation, and Article 38 VIS Regulation.

[132] European Digital Rights, *"Uses of AI in migration and border control: A fundamental rights approach to the Artificial Intelligence Act",* November 2021, available at https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf

transparency and data quality provisions may help, they cannot fully address the negative impact of these systems may have on TCNs seeking to enter the EU.

Arguably, the findings presented so far present several challenges for meaningful human intervention and adequate safeguards for TCNs subject to the ETIAS and VIS automated processing and highlight potential risks of discrimination and violation of the fundamental rights of TCNs. The lessons from the *Ligue des droits humains* judgment must be taken into consideration for enhancing safeguards for TCNs, and developing "properly functioning" human intervention mechanisms for visa and ETIAS applicants. Also, meaningful information about the envisaged processing operations must be communicated to TCNs with clear, plain language. In addition, accessible and convenient mechanisms must be developed for TCNs to allow them to contest the decision before the court or before the designated administrative body.

Section III – Conclusions

This paper has contributed to the reflections on the relationship between EU fundamental rights law and AI-enabled tools deployed in the border control domain. The focus has been the algorithm underpinning the ETIAS screening rules that will be driving the automated processing of applications submitted by visa and ETIAS applicants as from 2024. There is not yet enough publicity around the ETIAS screening rules and algorithm to conduct a thorough assessment; however, having regard to the legal framework and the process currently being followed to establish such rules, we deemed it appropriate to reflect on the fundamental rights risks of the ETIAS and VIS automated processing. We analysed the methodology for laying down the security, illegal immigration, and high epidemic risk indicators; the bias and distortions within the sets of characteristics identified so far; the responsibilities of the actors involved; the very likely opacity of the ETIAS screening rules and algorithms for human caseworkers; and the automation bias they may be subject to. In the light of this analysis, we argued that, despite the letter of the law, the ETIAS and VIS automated processing run the risk of leading to algorithmic outcomes that qualify as decisions based solely on automated means, within the meaning of Article 22 GDPR and Article 24 EUDPR. Our conclusion in based on a 'dynamic' and not literal reading of this provision, in line with the EDPB's Guidelines on Article 22, whereby, if a human decision is unable to scrutinise and challenge the merits of an automated outcome, this outcome is likely to be the decision itself, and hence lead to a prejudice for data subjects.

In order for this interpretation to be authoritative and drive policymaking, it will first need to find support in the case law of the Court of Justice dealing with future Article 22 GDPR / 24 EUDPR cases;[133] nonetheless, we believe it is the most reasonable reading of this provision in line with the objective to avoid escaping its underlying rationale, i.e., make sure that any algorithmic input to decision-making remains merely supportive and does not prejudice to any degree the human decision-maker's freedom to decide. Such reading is also in line with the EU's human-centric approach to AI regulation, which, however, for the time being, regrettably excludes AI systems deployed in EU border control systems from the scope of application of the proposed AI Act. The arguments put forward in this paper are meant to raise awareness on possibly underestimated risks of such AI systems and to spark reflections to identify suitable safeguards as early as possible. We believe it is all the more crucial to tackle such risks when considering that AI systems do not provide a full spectrum of their possible adverse effects until they are being used for a significant period of time.[134] Even AI systems that are embedded in a seemingly flawless workflow from a fundamental rights perspective may cause unforeseen damage

[133] And, in the law enforcement context, Article 11 LED.

[134] See Mittelstadt et al., cited *supra*, note 65, p. 2: "Identifying the influence of human subjectivity in algorithm design and configuration often requires investigation of long-term, multi-user development processes. Even with sufficient resources, problems and underlying values will often not be apparent until a problematic use case arises".

whose underlying causes are difficult to unravel. It therefore appears key to reduce as much as possible the range of risks to be dealt with upon entry into operation of the ETIAS and VIS AI systems. Well-grounded reflections to avoid the risk of solely automated decision-making are also likely to benefit user perception of automation at borders: Reduced opacity, awareness of thoroughly reviewed algorithmic outcomes, and meaningful possibility to challenge an adverse decision by ETIAS and VIS competent authorities, are likely increase trust amongst worldwide travellers in the overall EU border control and migration policy.