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

Jean Monnet Network on EU Law Enforcement
Working Paper Series

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

Lorenzo Gugliotta, Abdullah Elbi*

Abstract

In 2019 the EU laid down the regulatory groundwork for the 'interoperability' project in the Area of Freedom, Security and Justice. To make detection and analysis more effective, interoperability will rely on algorithmic tools that can qualify as 'AI systems' under the proposed AI Act. Due to the inherent risks posed by AI tools to non-discrimination and data protection, their use at borders will test the robustness of EU values and principles protecting third-country nationals in the migration and law enforcement context. However, AI tools used by EU interoperable migration databases may be excluded from the AI Act's scope. In our paper we acknowledge that this may be a source of concern given the fundamental rights impact of AI technologies especially when processing large amounts of data (including sensitive and biometric data) accessible across databases. These concerns warrant focusing on data protection law as possibly the main stronghold against violations of fundamental rights caused by the AI embedded in EU border and migration systems.

In this paper we apply the GDPR prohibition of purely automated decisions (Article 22) and the Court of Justice's case law on human control of automation to the use of AI technologies in the envisaged interoperability systems. As a case study, we focus on the AI-enabled processing envisaged under two EU border information systems, i.e., ETIAS and VIS, to vet third-country nationals applying for a travel authorisation or a Schengen visa, respectively. This processing was conceived to help competent authorities process the large amount of applicants' data and find patterns much more efficiently and quickly than humans could, while leaving to the authorities the power to take a final decision. This paper argues that, despite aiming to avoid decisions based solely on automated means, the ETIAS and VIS processing might inadvertently lead to automation 'taking over' the decision-making process. This would be the result of factors such as: insufficient transparency in the algorithm design; inherent biases in the statistics building the algorithm's basis; algorithmic opacity; and automation bias. We contrast the features of the ETIAS and VIS processing with a substantive reading of Article 22(1) GDPR (and Article 24(1) EU DPR), which should arguably not only prohibit decisions taken without any form of human involvement, but also decisions where human involvement was on substance meaningless. By favouring de facto AI-based profiling, and opening the door to informal 'rulebooks' in the decision-making process, the ETIAS and VIS processing may progressively reduce the extent to which human caseworkers review and question the AI-generated recommendations. Hence, they would risk sitting at odds with the prohibition in Article 22 GDPR. 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 trustworthy AI in the border and security ecosystem.

Keywords:

artificial intelligence; automated decision-making; automation bias; border management; data protection; fundamental rights; gdpr; migration; opacity

* 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. 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.

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 'interoperability' project in the Area of Freedom, Security and Justice. To make detection and analysis more effective, interoperability will rely on algorithmic tools that can qualify as 'AI systems' under the proposed AI Act. Due to the inherent risks posed by AI tools to non-discrimination and data protection, their use at borders will test the robustness of EU values and principles protecting third-country nationals in the migration and law enforcement context. However, AI tools used by EU interoperable migration databases may be excluded from the AI Act's scope. In our paper we acknowledge that this may be a source of concern given the fundamental rights impact of AI technologies especially when processing large amounts of data (including sensitive and biometric data) accessible across databases. These concerns warrant focusing on data protection law as possibly the main stronghold against violations of fundamental rights caused by the AI embedded in EU border and migration systems.

In this paper we apply the GDPR prohibition of purely automated decisions (Article 22) and the Court of Justice's case law on human control of automation to the use of AI technologies in the envisaged interoperability systems. As a case study, we focus on the AI-enabled processing envisaged under two EU border information systems, i.e., ETIAS and VIS, to vet third-country nationals applying for a travel authorisation or a Schengen visa, respectively. This processing was conceived to help competent authorities process the large amount of applicants' data and find patterns much more efficiently and quickly than humans could, while leaving to the authorities the power to take a final decision. This paper argues that, despite aiming to avoid decisions based solely on automated means, the ETIAS and VIS processing might inadvertently lead to automation 'taking over' the decision-making process. This would be the result of factors such as: insufficient transparency in the algorithm design; inherent biases in the statistics building the algorithm's basis; algorithmic opacity; and automation bias. We contrast the features of the ETIAS and VIS processing with a substantive reading of Article 22(1) GDPR (and Article 24(1) EU DPR), which should arguably not only prohibit decisions taken without any form of human involvement, but also decisions where human involvement was on substance meaningless. By favouring de facto AI-based profiling, and opening the door to informal 'rulebooks' in the decision-making process, the ETIAS and VIS processing may progressively reduce the extent to which human caseworkers review and question the AI-generated recommendations. Hence, they would risk sitting at odds with the prohibition in Article 22 GDPR. By analysing the implications of the AI-enabled

[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.

processing already envisaged in the current EU border regulation, the paper seeks to draw useful lessons for further adoption of trustworthy AI in the border and security ecosystem.

Keywords

artificial intelligence; automated decision-making; automation bias; border management; data protection; fundamental rights; gdpr; migration; opacity

1. 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] All over the world, countless initiatives have integrated AI technologies into border policies. They can be used in different settings and with varying degrees of sophistication and human oversight. Ever since the 2013 European Commission's Smart Borders Package,[5] the EU has 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.[6]

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 process enormous amounts of personal data of third-country nationals ('TCNs'). The operations entailed by the ETIAS and VIS involve 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 cross-links with other systems enabled by the interoperability architecture make these data processing operations all the more extensive and, potentially, invasive. The European Data Protection Supervisor ('EDPS'), 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.[7]

---

[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) <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> accessed 22 March 2023.

[4] See OECD, 'The Use Of Digitalisation And Artificial Intelligence In Migration Management' (February 2022) <https://www.oecd.org/migration/mig/EMN-OECD-INFORM-FEB-2022-The-use-of-Digitalisation-and-AI-in-Migration-Management.pdf> accessed 22 March 2023>.

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

[6] 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, OJ L 135; 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, OJ L 135.

[7] T Zandstra and E Brouwer, 'Fundamental Rights at the Digital Border: ETIAS, the Right to Data Protection, and the CJEU's *PNR* judgement' (2022) VerfBlog, p 3, DOI: 10.17176/20220624-162402-0 <https://verfassungsblog.de/digital-border/> accessed 22 March 2023>; EDPS, Opinion 3/2017 on the European Travel Information and Authorisation System (ETIAS), 7 March 2017, para 13, p 7 <https://edps.europa.eu/data-protection/our-work/publications/opinions/european-travel-information-and-authorisation-system_en> accessed 22 March 2023.

This paper focuses on 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. We first assess the extent to which the ETIAS and VIS automated processing are captured by the prohibitions to automated decision-making in EU data protection law. We focus on Article 22 of the General Data Protection Regulation (GDPR)[8] and Article 24 of Regulation 2018/1725[9] (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 (ie Frontex, or Frontex jointly with eu-LISA), or under the joint responsibility of Frontex and the Member States.

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,[10] interoperability,[11] as well as ETIAS,[12] the Entry/Exit System ('EES'),[13] VIS[14] and the Schengen Information System ('SIS')[15] individually. In terms of recent scholarly publications, Brouwer (2020)[16] assessed the necessity and proportionality of EU interoperability for borders and migration under data protection law; Blasi Casagran (2021)[17] focused on the challenges for various fundamental rights stemming from making EU border systems 'interoperable'; Vavoula (2021)[18] examined the fundamental rights implications of deploying AI systems at the EU borders; Zandstra and Brouwer (2022)[19] critically assessed the impact of ETIAS on the fundamental right to data protection; and most recently, Quintel (2022)[20] carried out a study connecting various data protection frameworks and their applicability to the EU borders and

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119.

[9] 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, OJ L 295.

[10] 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 <https://edps.europa.eu/data-protection/our-work/publications/opinions/eu-smart-borders-package_en> accessed 22 March 2023.

[11] FRA Opinion, Interoperability and fundamental rights Implications, 18 April 2018 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-01-2018-interoperability_en.pdf> accessed 22 March 2023.

[12] EDPS, Opinion 3/2017, cited *supra,* n 7; FRA Opinion 2/2017, The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS), 10 July 2017 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-opinion-02-2017-etias.pdf> accessed 22 March 2023.

[13] EDPS Opinion on the SBP and the revised EES proposal, cited *supra,* n 10.

[14] EDPS Opinion 9/2018 on the Proposal for a new Regulation on the Visa Information System, 12 December 2018 <https://edps.europa.eu/data-protection/our-work/publications/opinions/upgrading-visa-information-system-vis_en>. accessed 22 March 2023; FRA Opinion, The revised Visa Information System and its fundamental rights implications, 7 September 2018 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-visa-information-system-02-2018-corr_en.pdf> accessed 22 March 2023.

[15] EDPS Opinion 7/2017 on the new legal basis of the Schengen Information System, 2 May 2017 <https://edps.europa.eu/data-protection/our-work/publications/opinions/schengen-information-system-new-legal-basis_en> accessed 22 March 2023.

[16] E Brouwer, 'Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection' 26 (1) (2020) European Public Law 71-92 <https://doi.org/10.54648/euro2020005>.

[17] C Blasi Casagran, 'Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU' 21 (2021) Human Rights Law Review, 433-457 <https://doi.org/10.1093/hrlr/ngaa057>.

[18] N Vavoula, 'Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' 23 (2021) European Journal of Migration and Law 457-484 <https://doi.org/10.1163/15718166-12340114>.

[19] T Zandstra and E Brouwer, cited *supra,* n 7.

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

migration ecosystem; Derave et al (2022)[21] took the ETIAS automated processing as a case study to demonstrate their potential discriminatory effects; in the same vein, Eklund (2022)[22] 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 under the GDPR. For instance, Veale and Edwards (2018)[23] critically assessed the 29WP Guidelines on Article 22 GDPR; González and de Hert (2019)[24] discussed that provision in connection with GDPR-based lawful grounds for processing; Malgieri (2019)[25] focused on the safeguards for data subjects, especially in terms of explainability of decisions; Sancho (2020)[26] provides an in-depth analysis of Article 22 gauged towards enhanced protection of individuals; de Hert and Lazcoz (2021)[27] sought to 're-purpose' Article 22 within a more dynamic human oversight ecosystem vis-à-vis automated decision-making; and Binns and Veale (2021) crafted a framework for assessing various decision-making structure through the lens of Article 22.[28]

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. 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.

2. 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.

A. ETIAS and VIS within Interoperability

ETIAS and VIS contribute, along with other systems, to national and EU migration, border control and internal security policies. ETIAS was established in 2018 with Regulation 2018/1240[29] and, according

[21] C Derave, N Genicot, and N Hetmanska, 'The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System' 13 (2022) European Journal of Risk Regulation (2022) 389–420 <https://doi.org/10.1017/err.2022.5>.

[22] AM Eklund, 'Frontex and 'Algorithmic Discretion' (2022), DOI: 10.17176/20220910-110512-0 <https://verfassungsblog.de/frontex-and-algorithmic-discretion-part-i/> accessed 22 March 2023>.

[23] M Veale and L Edwards, 'Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling', 34 (2018) Computer Law & Security Review 398-404 <https://doi.org/10.1016/j.clsr.2017.12.002>.

[24] E Gil González and P de Hert, '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 <https://doi.org/10.1007/s12027-018-0546-z> accessed 22 March 2023>.

[25] G Malgieri, 'Automated decision-making in the EU Member States: The right to explanation and other 'suitable safeguards' in the national legislations', 35 (2019) Computer Law & Security Review <https://doi.org/10.1016/j.clsr.2019.05.002>.

[26] D Sancho, '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), 136-156 <https://doi.org/10.1017/9781108347846.005>.

[27] P De Hert, and G Lazcoz Moratinos, 'Radical rewriting of Article 22 GDPR on machine decisions in the AI era' (2021) European Law Blog <https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/> accessed 22 March 2023>.

[28] R Binns and M Veale, 'Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR' 11 (4) (2021) International Data Privacy Law <https://doi.org/10.1093/idpl/ipab020>.

[29] 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, OJ L 236.

to eu-LISA's latest plans, is set to enter operations in 2024.[30] It is meant to collect and process the data of visa-exempt third-country nationals (VE-TCNs)[31] who intend to travel to the Schengen Area for a short term. VIS was established in 2004,[32] entered operations in 2011, and since then 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,[33] subsequently reviewed and recast on several occasions including the 2021 VIS Recast,[34] which enlarged its scope to include long-stay visas and residence permits.[35] 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 designed to be integrated within the EU's Interoperability framework.[36] 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.

B. 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.

Under the ETIAS Regulation, once it receives a new application by a TCN and records the applicant's data, the ETIAS Central System will verify, 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. The system then applies screening rules and risk indicators to the applicant's data (see more on this below).[37] Subsequently, for any match found during the first step, ETIAS will create a 'hit', ie will flag the existence of a match or an outcome that should be analysed further. If no hits are created, ETIAS will then automatically grant the applicant an electronic travel authorisation with no human involvement; if, by contrast, one or more hits are created, the application file is up for manual processing pursuant to Articles 22 and 26 of the ETIAS Regulation, which will lead to a human decision to grant or refuse the travel authorisation.

Figure 1: ETIAS workflow

[30] See 'Why was ETIAS delayed again to 2024?' <https://etias.com/articles/why-was-etias-delayed-again-to-2024> accessed 22 March 2023.

[31] 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).

[32] 2004/512/EC: Council Decision of 8 June 2004 establishing the Visa Information System (VIS).

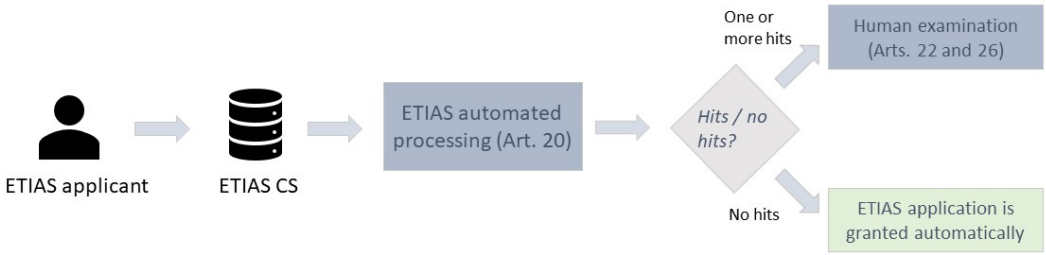
[33] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ L 218.

[34] Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System, OJ L 248.

[35] 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) <https://www.eulisa.europa.eu/Publications/Reports/2021%20VIS%20Report.pdf> accessed 22 March 2023>.

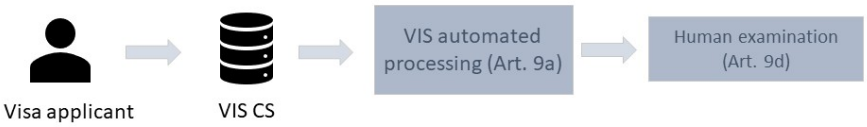
[36] See European Commission, Proposal for Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 (COM(2017) 793 final), 2017/0351 (COD), p 3.

[37] The list of comparisons to be carried out by the ETIAS Central System is laid down in Art 20(5) ETIAS Regulation.



The VIS process is similar but not identical. Upon recording the visa applicant's data, the VIS Central System will cross-check data as ETIAS will, and will apply the same risk indicators as under ETIAS to the application file. Then, VIS will create hits for any matches. Now – and here is where VIS differs from ETIAS – regardless of whether any hit is created, the visa application file will be manually reviewed by the competent visa authority to decide whether to grant a visa or not.

Figure 2: VIS workflow



Under ETIAS, the system is authorised to issue a travel authorisation in the 'no-hit' scenario; conversely, the visa framework always entrusts the competent authority with issuing a visa. This distinction, which stems from the different average risk profile that VE-TCNs and VH-TCNs are believed to carry from a migration and security policy perspective,[38] 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.

Here it is appropriate to make one key terminological remark. By 'automated processing' 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. 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,[39] whether he or she has replied affirmatively to certain questions,[40] or whether he or she has data recorded in other information systems.[41] 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, the research focuses on those specific data processing operations whereby the system is expected to apply criteria and indicators to an individual situation and derive non-trivial outcomes from it. This is the case of the following two provisions:

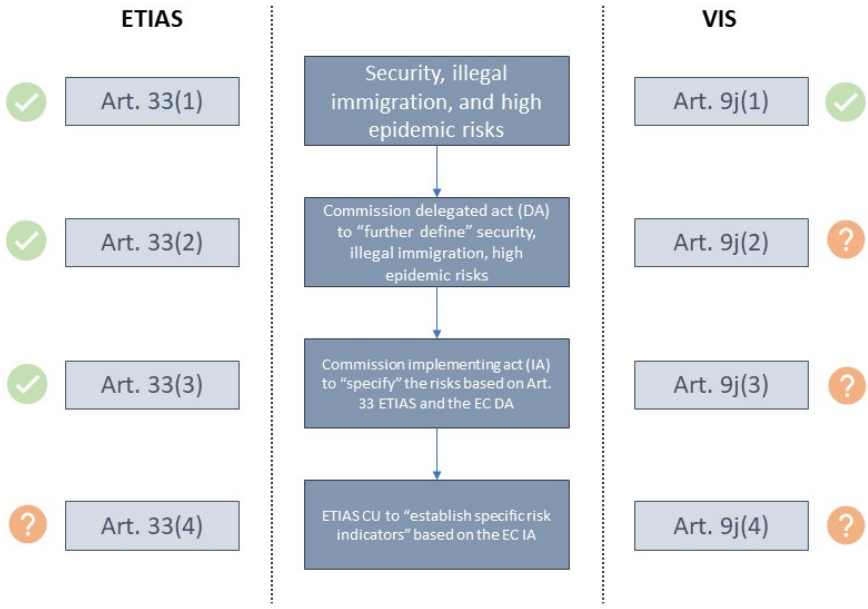
[38] See implicitly Recital 9 of the ETIAS Regulation.
[39] Eg Art 20(2)(m) ETIAS Regulation.
[40] Eg Art 20(3) ETIAS Regulation.
[41] Eg Art 20(2) ETIAS Regulation.

- 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, 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.[42] The indicators shall be established by the ETIAS CU (Frontex) based on a complex series of generic and specific risks. The high-level risks – ie 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,[43] which was adopted in 2021;[44] subsequently, the Commission shall, via an implementing act, specify the risks mentioned in the ETIAS Regulation and those defined in the delegated act;[45] finally, the ETIAS CU shall use all these regulatory sources to establish the risk indicators[46] to be used by the ETIAS screening rules. An identical method was introduced into the VIS Regulation.[47]

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.

[42] See Arts 33 ETIAS Regulation and 9j VIS Recast Regulation.
[43] Art 33(2) ETIAS Regulation.
[44] Commission delegated decision of 23 November 2021 on further defining security, illegal immigration or high epidemic risks. C(2021) 4981 final.
[45] Art 33(3) ETIAS Regulation.
[46] Art 33(4) ETIAS Regulation.
[47] Arts 9j(2) and 9j(3) VIS Regulation, as amended by Regulation (EU) 2021/1134.

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

Due to confidentiality of information and to the ongoing law-making process, 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.'[48] The act defines 'sets of characteristics' 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.'[49] 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, country and city of residence. Nationality and residence are dimensions that 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 deriving the person's ethnic origin.[50] 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 appears that the ETIAS and VIS delegated acts, instead of further defining the risks, merely detail additional parameters for statistical analysis and 'pass the hot potato' (ie *actually* define the risks) back to the ETIAS CU. This is particularly worrying because under the ETIAS and VIS Regulations the risk indicators will be established by the ETIAS CU, ie will be set unilaterally by an executive body outside the constraints and safeguards of the rules of procedures on law-making. It

[48] C(2021) 4981 final, Recital 3.

[49] Ibid., Art 2(b).

[50] With regard to the VIS Delegated Act, see EDPS, 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, para 15 <2022-0917_d2423_formal_comments_en.pdf (europa.eu)>. In the same vein see also EDPS, Opinion 3/2017, cited *supra,* n 7, 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, Judgement of the Court (Grand Chamber) of 1 August 2022, *OT v Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601, para 125.

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 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 *Ligue des droits humains* judgement.[51] Such rule-making practice is likely to make the whole system even more opaque 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 […]'.[52] 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 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 a heightened difficulty in reviewing the substance of algorithmic outcomes and thus in determining, for instance, *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.'[53] As will become apparent in Section II, 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 human reviewers 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.[54]

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

A. 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.'[55] Such a decision, commonly but non unanimously seen as outright prohibited to data controllers,[56] can nonetheless be allowed (i) if it is necessary for entering

[51] C-817/19, *Ligue des droits humains v Conseil des ministres*, judgement of 21 June 2022, ECLI :EU :C :2022 :491, para 195. With regard to the pre-determined criteria mentioned in the PNR Directive, the Court observed that '[…] given the opacity which c9haracterises 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 […]'.

[52] J Burrell, 'How the machine "thinks"': Understanding opacity in machine learning algorithms' 3 (1) 2016) Big Data & Society <https://doi.org/10.1177/2053951715622512>.

[53] J Burrell, cited *supra,* n 52., p 2.

[54] BD Mittelstadt, P Allo, M Taddeo, S Wachter, and L Floridi, 'The ethics of algorithms: Mapping the debate' 3 (2) (2016) Big Data & Society <https://doi.org/10.1177/2053951716679679>.

[55] Art 22(1) GDPR.

[56] See for instance, arguing for the prohibition approach, D Sancho, cited *supra*, n 26. For an opposite view, which qualifies the statement of Art 22(1) GDPR as a right to be exercised by the data subject, see L Tosoni, 'The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation', 11 (2) (2021) International Data Privacy Law <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3845913>.

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.[57] The provision of Article 24 EUDPR is essentially identical.

The reading of the first two paragraphs of Articles 22 GDPR and 24 EUDPR implies 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 (ie, the ETIAS and VIS Regulations) do not lay down sufficient safeguards for the data subjects. We analyse each condition separately.

B. 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, ie if the automated processing does not trigger any hits the system grants the travel authorisation automatically. In no other case does the processing lead to an unchecked outcome. 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.[58]

The issue with this conclusion is that the intervention of human reviewers, formally provided for by the law, may actually not be enough to rule out a decision with legal or similarly significant adverse effects on data subjects.

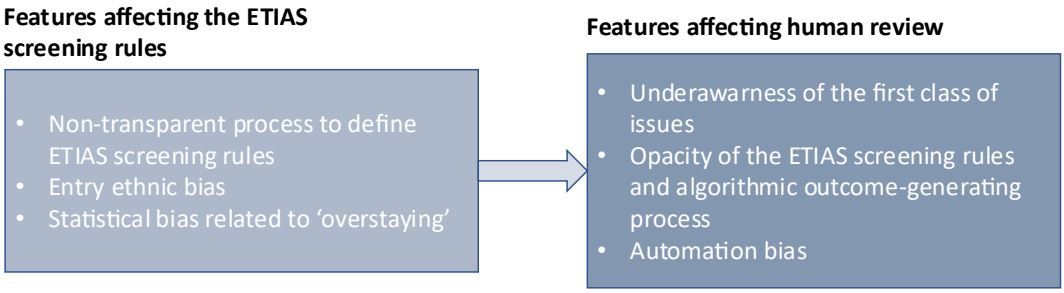
The risk of running afoul of Article 22 GDPR / 24 EUDPR would essentially depend on the relative weight of the outcome of the automated processing and the human review. The problem may reside in the non-substantial nature of the human review at hand. Being aware of such possibility, the 29WP writes in its Guidelines on Article 22 that 'The controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture.'[59] Of course, it is not easy to ascertain *in abstracto* whether human intervention is merely formalistic: the practice may also be necessary to a comprehensive assessment. Alternatively, we can imagine that the human intervention is initially substantial, but its real weight gets thwarted in the long run by the so-called 'automation bias'. 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 meaningfully scrutinise 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 may pose a risk of non-meaningful human review that may be reinforced by automation bias going forward, thereby possibly generating outcomes that would qualify as decisions based solely on automated means.[60] The figure below collects the features that, combined, may cause these effects. We distinguish between a) features that occur when the automated process is running; and b) features that are inherent to the

[57] Ibid., para 2.
[58] See for instance Derave et al, cited *supra,* n 21, p 408.
[59] 29WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p 21, <https://ec.europa.eu/newsroom/article29/items/612053> accessed 22 March 2023.
[60] See also T Zandstra and E Brouwer, cited *supra,* n 7, p 3.

ETIAS screening rules but that prevent or limit the human caseworkers' ability to meaningfully review and challenge the automated outcome *ex-post*.

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

Two of the features in the first category are examples of *bias*. Before delving into them, it is worth noting that algorithms make biased outputs by default, by their very nature.[61] This is because any algorithm originates from a design and configuration established by humans, whose priorities and values inevitably shape the algorithm's rules and functioning logic at the outset. These determine a design *choice* amongst other possibilities.[62] 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 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'

By 'ethnic entry bias' we 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[63] 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 insofar as 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 […]'[64] 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 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 be a hidden distortion competent authorities would have a hard time detecting and correcting.

Statistical bias

Statistical bias 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

[61] Mittelstadt et al, cited *supra,* n 54, p 7.
[62] 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.'
[63] European Union Agency for Fundamental Rights, *Fundamental Rights at Airports: Border Checks at Five International Airports in the European Union* (2014) 45.
[64] Art 33(2)(c) ETIAS Regulation.

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.[65] 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. 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. Scholars have highlighted that statistical methods do not necessarily highlight causal connections between inputs and may not provide sufficiently conclusive evidence for decision-making.[66] The example of an AI-based law enforcement tool deployed in a British police force, the Harm Assessment Risk Tool ('HART'),[67] 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, they call for more police attention and hence for an ever-increasing spotlight.[68] 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.

The key problem with this outcome 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 it nor ability to correct the overall decision-making process. In the ETIAS example, 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 opacity and automation bias (see below) self-reinforce, 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.

---

[65] Art 2(3) EES Regulation does exclude from its scope of application 'holders of residence permits' listed in Art 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 et al., cited *supra, n* 21, pp 413-14.

[66] Mittelstadt et al, cited *supra,* n 54.

[67] Developed for the Durham Constabulary in cooperation with Cambridge University <https://www.cam.ac.uk/research/features/helping-police-make-custody-decisions-using-artificial-intelligence> accessed 22 March 2023.

[68] M Oswald, J Grace, S Urwin, and GC Barnes , 'Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality' 27 (2) (2018) Information & Communication Technology Law, p 228 <https://doi.org/10.1080/13600834.2018.1458455>.

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.[69] 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 is that human reviewers (ie visa authorities and ETIAS NUs) are not or insufficiently aware of the above-mentioned features. This problem may well be amplified by a lack of understanding and training. In the context of a the 'HART' 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.[70] 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'.[71]

Opacity of the ETIAS screening rules and of the algorithm

Possibly the most crucial feature of the ETIAS and VIS automated processing is the opacity behind the 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,[72] 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 (ie 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);[73] 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.'[74] Depending on how the risk indicators and the screening rules are designed to work, they may or may not be granular enough to show 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.[75] 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

[69] Derave et al, cited *supra,* n 21, p 415-417. See also FRA, Opinion 2/2017, cited *supra,* n 12, p 29; FRA, 'Getting the future right: Artificial intelligence and fundamental rights' (2020), p 11, <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights> accessed 22 March 2023>. N Vavoula, cited *supra*, n 18., pp 464-65: '[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.

[70] Oswald et al, cited *supra,* n 68, p 234.

[71] J Burrell, cited *supra,* n 52, p 4.

[72] CJEU, Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, ECLI:EU:C:2017:592.

[73] Ibid., para 172.

[74] Ibid., para 173.

[75] Derave et al, cited *supra,* n 21.

risk indicators. The [competent authority] shall *individually* assess the security, illegal immigration and high epidemic risks in all cases' (emphasis added).[76]

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 assessed by the algorithm. Because of the first flaw, the criteria that triggered the hit(s) may be too generic 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.'[77]

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. 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, ie 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. At the outset, we observe that ''*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

[76] Art 20(5) ETIAS Regulation; Art 9c(6) VIS Regulation.
[77] EDPS, Opinion 3/2017, cited *supra,* n 7, para 37, p 11.

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.[78] 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;[79] but if the human filter is devoid of substance, we run 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'

The impact of opacity on decision-makers' ability to prevent decisions based solely on automated means can be reinforced by another factor: automation bias. This type of bias affects the human review process in practice, rather than 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',[80] 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.'[81]

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 ('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 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

[78] See Oswald et al, cited *supra,* n 68, 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.'

[79] More generally, no information does 'necessarily imply the attribution of meaning, as it may in the case of humans', see M Hildebrandt, 'Law As Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics' (2017) p 10, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2983045> accessed 22 March 2023; see also N Silver, 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', N Silver, *The Signal and the Noise: The Art and Science of Prediction* (Penguin 2013).

[80] Oswald et al, cited *supra,* n 68, p 232.

[81] Ibid., p 225. See in this respect D Beer, 'The social power of algorithms' 20 (1) (2017) Information, Communication & Society, pp 10-11 <https://doi.org/10.1080/1369118X.2016.1216147>.

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 human review. The result may be the creation of 'informal rulebooks', ie 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: 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 additionally affect caseworkers already potentially subject to automation bias for a particular set of characteristics.

Second, we submit there is also a *time-related challenge*. 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 input the data or have useful information to review the hit.[82] 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- reach independent decisions on each hit related to security, illegal immigration, and high epidemic risk. 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.[83]

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.

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?[84] It may be that the algorithm supporting the ETIAS screening rules does not, as such, possess learning capabilities. However, the Commission and eu-LISA have reported to envisage an increasing role for AI in the border control and migration contexts.[85] To the extent that the ETIAS and VIS algorithm are planned to be upgraded in the future, there should be a 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.

C. Condition II – Safeguards for data subjects

Provided that condition I is met, Article 22 GDPR and Article 24 EUDPR would require adequate safeguards for TCNs' rights and freedoms to allow ETIAS and VIS automated processing. This is especially pertinent considering that such processing might infringe several fundamental rights, such as the right to private and family life,[86] the right to personal data protection,[87] the right to an effective

[82] For instance, Arts 26(3), 28 ETIAS Regulation.
[83] Arts 30 and 32 ETIAS Regulation.
[84] See MS Gal, 'Algorithmic Challenges to Autonomous Choice', 25 (1) (2018) Michigan Technology Law Review, p 6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2971456>.
[85] eu-LISA, 'Artificial Intelligence in the Operational Management of Large-scale IT Systems: Perspective for eu-LISA', Research and Technology Monitoring Report (July 2020).
[86] Art 7 of the EU Charter of Fundamental Rights.
[87] Ibid., Art 8.

remedy and to a fair trial.[88] 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[89] and reiterated in *Ligue des droits humains* judgement,[90] 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'.[91] 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 provide sufficient safeguards because the ETIAS CU merely 'verifies' formal features of the processing and transfers the hit to the ETIAS NU.[92] 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 ETIAS NU 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.[93] However, as explored in Section II, the envisaged human intervention mechanism may be hindered by the opacity of the pre-determined criteria and automation bias.[94]

Pursuant to Article 8(3) ETIAS and, Member States are obliged to provide the ETIAS NUs with adequate resources (including training) to fulfil their tasks in accordance with the deadlines set out in this Regulation. 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.[95] This principle might be integrated in the various Handbooks prepared by the European Commission *inter alia* for border authorities.

---

[88] Ibid., Art 47. See also 29WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p 27.

[89] Opinion 1/15, cited *supra*, n 72.

[90] *Ligue des droits humains*, para 203.

[91] Ibid., para 123.

[92] Art 22(4) ETIAS Regulation mandates the deletion of false positives. Under Art 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.

[93] Art 9 VIS Regulation.

[94] AM Eklund, cited *supra,* n 22.

[95] 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, <https://www.weforum.org/reports/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case-law-enforcement-investigations-revised-2022> accessed 22 March 2023.

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, they 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[96] 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, 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.[97]

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 struggle to understand 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 understand the reason why a given program arrived at a positive match'.[98] 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'.[99] 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'.[100]

Other safeguards

Article 10 ETIAS Regulation establishes an independent ETIAS Fundamental Rights Guidance Board[101] 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 publish annual reports that may contribute to transparency and reduce the informational asymmetry of data subjects.

---

[96] In particular, the information on the procedures for exercising the rights under Arts 13 to 16 of Regulation (EC) No 45/2001 and Arts 15 to 18 GDPR.

[97] Arts 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 T Quintel, cited *supra*, n 20.

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

[99] Ibid., para 195.

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

[101] Art 10 ETIAS Regulation is included following the study for the LIBE committee: European Parliament, Directorate-General for Internal Policies, Policy Department C – Citizens' Rights and Constitutional Affairs, 'European Travel Information And Authorisation System (ETIAS): Border Management, Fundamental Rights And Data Protection' (2017), <https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583148/IPOL_STU(2017)583148_EN.pdf> accessed 22 March 2023. 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.'

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. All TCNs whose data is processed in the context of ETIAS and VIS automated processing are accorded specific rights.[102] 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'), 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.[103] Overall, this could lead to significant and harmful decisions such as detention and deportation, which could have a profound impact on TCNs. While 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* judgement must be applied to enhance safeguards for TCNs, and develop '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.

4. 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

[102] Art 38 ETIAS Regulation, and Art 38 VIS Regulation.

[103] European Digital Rights, 'Uses of AI in migration and border control: A fundamental rights approach to the Artificial Intelligence Act' (November 2021) <https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf> accessed 22 March 2023.

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; nonetheless, we believe it is the most reasonable reading of this provision in line with the objective to avoid escaping its underlying rationale, ie 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.[104] Even AI systems that are embedded in a seemingly flawless workflow from a fundamental rights perspective may cause unforeseen damage 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.

Competing interests

The authors have no conflicts of interest to declare.

[104] See Mittelstadt et al, cited *supra,* n 54, 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'.