Computer Law & Security Review 54 (2024) 105995

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Prospective implementation of ai for enhancing European (in)security: Challenges in reasoning of automated travel authorization decisions

Erzsébet Csatlós

Institute of Public Law, University of Szeged, Faculty of Law and Political Sciences, H-6721 Szeged, Bocskai u. 10-12., Hungary

ARTICLE INFO

Keywords:
Automated decision-making
Travel authorisation
Reasoning
Security threat

ABSTRACT

The *European Travel Information and Authorisation System*, along with the automated decision-making system for immigration filtering, is soon to become a guardian controlling entry into Europe. In the digital realm of issuing travel authorisations, a central question arises: does streamlining the process of using an authoritative decision through IT tools and artificial intelligence simplify administrative decision-making, or does it raise more profound legal issues? The pressing question is whether algorithms will ultimately determine human destinies, or if we have not reached that point yet. This paper examines the set of rules for making a decision on the refusal of a travel permit, considering the obligations tied to providing *reasons* for such decisions. It emphasizes that the rationale should be built upon a combination of factual and legal foundations, which would entail revealing data linked to profiling. While explicit rights for explanations might not be granted, having substantial information gives the ability to contest decisions. To ensure decisions are well-founded, the methodology used for profiling must support these determinations, as general system descriptions are inadequate for clarifying specific cases. Therefore, the paper concludes that the complex interaction between the ETIAS screening process, data protection laws, and national security concerns presents a challenging situation for procedural rights. Fundamental rights, such as accessing records and receiving decision explanations, clash with the necessity to safeguard national security and build a so-called security union for Europe, it establishes a feeling of insecurity about respect for EU values.

1. Introduction

Migration control has posed a persistent challenge within the European Administrative Space over an extended period. Because of its classification as a security concern,[1] the European Union (EU) often addresses immigration as both a crisis and a security peril.[2] This approach contributes to the intricate nature of immigration management.[3] As a result, the administrative workload is substantial, given the involvement of millions of individual cases. By January 1st, 2022, approximately 23.8 million non-EU citizens were residing in EU Member States, comprising 5.3 % of the EU's total population.[4] Also, annually, there are several tens of thousands of third-country nationals that are refused entry, found to be illegally present, ordered to leave or returned to leave.[5]

E-mail address: csatlos.e@juris.u-szeged.hu.

[1] Monika Wohlfeld, 'Is Migration a Security Issue?' in Grech, O. and & Wohlfeld, M. (eds), *Migration in the Mediterranean: human rights, security and development perspectives*, 61 (MEDAC, Msida 2014).

[2] Communication from the Commission COM(2016) 205 final, Stronger and Smarter Information Systems for Borders and Security [2016] 2.

[3] James Cardwell, 'Tackling Europe's Migration 'Crisis' through Law and 'New Governance' (2018) 9(1) Global Policy 67, 73.

[4] Migration and migrant population statistics. Data extracted in March 2023. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Migration_and_migrant_population_statistics#Migrant_population:_23.8_million_non-EU_citizens_living_in_the_EU_on_1_January_2022 accessed 20 August 2023.

[5] *Annual Report on Migration and Asylum 2022.* Statistical Annex Co-produced by Eurostat and the European Migration Network. European Union, Luxembourg, 2023. 22-23.

https://doi.org/10.1016/j.clsr.2024.105995

Available online 4 June 2024

Information is power, and there were many available data on a person even on third-country nationals (TCN)[6] to exploit and make use of them when first a better view on immigration emerged. Also, to address the immense caseload of immigration comprehensively and establish a cohesive system, a digitalization strategy is being pursued in the form of a 'technological risk filter',[7] leveraging the interoperability of existing resources.[8] This involves the collection of personal data and the utilization of databases through collaborative endeavours encompassing border management, criminal cooperation, and migration control policies. Through this, collaborative approachthere is an envisaged bridging of the gap in monitoring and regulating the influx of visa-exempt TCNs.

The world is divided by EU migration rules: there are third-country nationals who may come to Europe without any concerns (whitelisted TCN), and there are nationals from other countries who are obliged to acquire a visa (blacklisted TCN) even for a short stay. Therefore, the latter group must undergo an authority procedure through which, among other considerations, their potential nature as a threat to European security might be assessed on a case-by-case basis by the competent authorities of the Member State of destination.[9] Expanding this verification process for both types of short-term travellers would entail a significant workload. Thus, the *European Travel Information and Authorisation System* (ETIAS) platform represents a digital solution that allows for the execution of this task in a rather unconventional manner. Unlike relying on the administration of individual Member States, ETIAS centralizes the process of granting travel authorizations by the screening of potentially risky elements, involving Member State administration only when procedural guarantees necessitate such involvement.[10]

Under the context of an aspirational *effective and genuine European security union* concept by the Commission,[11] the ETIAS system is designed to automatically process online applications and decide upon travel authorizations for visa-exempt TCNs for short stays. Its purpose is to ascertain that the presence of these individuals within Member States' territories *does not, and will not, endanger security, lead to illegal immigration, or pose a substantial epidemic risk based on concrete factual evidence and an assumption of the circumstances*. The issuance of a travel authorization therefore signifies a decision affirming the absence of concrete indications or reasonable grounds to suspect that the individual's presence within EU territories carries potential risks. However, there are debates on the serious nature of the relationship between immigration and crime,[12] the ETIAS aims to focus on gaining and exploiting already existing data on short-term visitor TCNs to the ETIAS countries. A crucial question arises regarding what a security union means by this: what can be achieved through data collection and analysis resulting in the denial of entrance that current control of border management, law enforcement, and migration cannot? The EU lacks jurisdiction over security-related legal harmonization and must also respect essential state functions, including maintaining law and order and safeguarding national security, as these are the sole responsibilities of Member States.[13] Thus, what may be the outcome of data collection and profiling that effectively supplements a secure environment *for everyone* in the rapidly changing European security threat landscape, as envisioned by the *EU Security Union Strategy*? Specifically, how can security policy remain grounded in common European values, respecting and upholding the rule of law, equality, and fundamental rights, while guaranteeing transparency, accountability, and democratic control as it is proclaimed? All in all, the pressing question is whether algorithms will ultimately determine the legal situation of TCNs and therefore human destinies, or if we have not reached that point yet.

The system launch has been consistently delayed, but since the ETIAS regulation was established in 2018, it has given rise to numerous questions.[14] This study aims to explore whether algorithms have the power to determine legal status related to immigration, focusing on the legal aspects of automated decision-making within the EU framework. It examines how fundamental values promoted by the EU intersect with automated decision-making procedures. Since the legality of administrative decisions is manifested in the reasoning behind those decisions, this forms the centre of the analysis: how the decisions on travel authorisation are made and on what basis they are issued. The primary emphasis lies on fact-finding and evidentiary considerations, particularly in cases where travel authorization is denied, as procedural safeguards gain significance when they impact individuals adversely. Moreover, the quality of decisions and their underlying rationale directly affect the efficacy of legal recourse. Therefore, the central research question revolves around how procedural guarantees within authority procedures can be reinterpreted within a highly digitalized decision-making framework. Despite the emphasis on principles like necessity, proportionality, and legality to protect individuals, especially the most vulnerable as per the EU Security Union Strategy, the procedure appears to be filled with uncertainty, potentially amplifying insecurity due to perceived arbitrariness.

[6] *Under watchful eyes: biometrics, EU IT systems and fundamental rights* (European Union Agency for Fundamental Rights, 2018) 9; Teresa Quintel, 'Connecting personal data of Third Country Nationals Interoperability of EU databases in the light of the CJEU's case law on data retention' (2018) University of Luxembourg Law Working Paper No. 002. 5-9.

[7] Amanda Musco Eklund, Rule of Law Challenges of 'Algorithmic Discretion' & Automation in EU Border Control. A Case Study of ETIAS Through the Lens of Legality' (2023) 25(3) European Journal of Migration and Law 251.

[8] For interoperability, the European Search Portal (ESP), the Common Biometric Matching Service (BMS), the Common Identity Repository (CIR) and the Multiple Identity Recognition System (MID) were created. European Parliament and Council Regulation (EU) 2019/817 of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA [2019]. OJ L 135/27, Article 6.

[9] European Parliament and Council Regulation (EU) 2018/1806 on listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement (codification) [2018] OJ L303/39. Annex I and II; Maarten den Heijer, 'Visas and Non-discrimination' (2018) 20(4) European Journal of Migration and Law 480.

[10] *Cf.* European Parliament and Council Regulation (EU) 2016/679 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 OJ L 119/1 [2016] [hereinafter: GDPR] Article 22.1. and 3.

[11] Communication from the Commission COM/2020/605 final on the EU Security Union Strategy [2020] Brussels [hereinafter: EU Security Union Strategy] 2.

[12] COM(2016) 205 final 2.; Standard Eurobarometer 85- Spring 2016 Europeans' views on the priorities of the European Union https://europa.eu/eurobarometer/surveys/detail/2130 accessed 03 January 2024, 51; Standard Eurobarometer 87 – Spring 2017 Europeans' views nt he priorities of the European Union; https://europa.eu/eurobarometer/surveys/detail/2142 accessed 03January 2024, 47; Standard Eurobarometer 89 – Spring 2018 The views of Europeans on the European Union's priorities https://europa.eu/eurobarometer/surveys/detail/2180 accessed 03 January 2024, 37 *cf. The alleged relationship between immigration and criminality (*2022) Openpolis (REC 2014-2020) https://www.openpolis.it/wp-content/uploads/2022/06/The-alleged-relationship-between-immigration-and-criminality.pdf accessed 03 January 2024.

[13] EU Security Union Strategy 1; 2-5.

[14] Regarding current information, the travel authorization for visa-exempt travellers entering Europe is expected to be introduced in mind-2025. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/european-travel-information-authorisation-system_en accessed 03January 2024.

2. The structure of the system and the decision-making process

The primary objective of ETIAS is to strengthen security measures, counteract unlawful immigration, and uphold public health by evaluating prospective visitors *before* they arrive at external border entry points.[15] Visa-exempt TCNs will need to complete an online application form via the official public website or a designated mobile application well in advance of their intended travel. Alternatively, if they are already present within a Member State's territory, they must apply before their existing travel authorization expires. It is anticipated that most applications will receive automated approval, resulting in travel authorization being granted within seconds *(automated decision on travel permit)*.[16] The travel authorisation system is built on the collaboration of the direct and indirect administration of the multilevel European administration as modelled in Fig. 1. where the major role is played by the direct administration represented by the ETIAS Central System and the Member State administration (indirect administration) is aimed to serve a subsidiary role.

2.1. Sharing of tasks and competencies among the levels of European administration

The functioning of the ETIAS relies on the collection and retention of individual data, encompassing historical activities and specific attributes, to assess an individual's eligibility for travel authorization. This centralized system enhances efficiency and effectiveness in addressing security risks linked to migration to the EU, all while adhering to consistent standards. As you can see in Fig. 1, once the applicant fills out the online form and the system detects it as completed, a claim file is initiated to be processed. Throughout the application process, the personal information provided by applicants is cross-referenced with records, files, and alerts in various EU databases and information systems (*data collection and verification phase of automated processing*). The ETIAS screening rules are essentially algorithms that facilitate profiling.[17] In this context, the *infrastructural skeleton*[18] for verifying visa-exempt third-country nationals is the ETIAS Central System. This system manages the processing and retention of data submitted via ETIAS applications, as well as the comparison of this data against multiple EU and international databases and watchlists (*database checks and biometric data analysis phase of automated processing*).

The applicant's data is compared against various databases to identify any potential risks or concerns. As shown in Fig. 1, there are three groups of datasets to consult: the databases, the ETIAS watchlist, and the specific risk indicators, all related to TCNs but in distinct manners. The databases under the scope of the system are those that *ab ovo* store data on TCNs *Schengen Information System* (SIS), the *Visa Information System* (VIS), Eurodac, the soon-to-up Entry/Exit System (EES), Europol data, *Interpol Stolen and Lost Travel Document database* (SLTD), *Interpol Travel Documents Associated with Notices* database (TDAWN). The ETIAS watchlist will serve as a significant tool for identifying potential connections between the information furnished in an ETIAS application and data on individuals who are under suspicion of involvement in terrorist acts or other severe criminal activities. Data should be entered into the ETIAS watchlist by Europol, and by Member States.[19] Transitioning from concrete data to more speculative projections of an individual's future conduct, the *specific risk indicators* will function as a broad screening mechanism. It will constitute a collection of factors subject to regular oversight and updates, will be formulated, instituted, evaluated in advance, put into action, retrospectively assessed, modified, and removed by the ETIAS Central Unit. This process will involve consultations with an ETIAS screening board comprised of delegates from the ETIAS National Units and pertinent agencies to improve the system in *pattern recognition, intelligence sharing and continuous learning*. The Commission is authorized to adopt a delegated act that elaborates on the risks associated with security, illegal immigration, or a high epidemic risk. This elaboration will be based on various information available to the Commission. These particular risk indicators will be defined, established, assessed in advance, implemented, evaluated afterwards, and subject to revision or removal by the ETIAS Central Unit. This process will take place following consultation with the ETIAS Screening Board.[20] Hence, the decision-making process will rely on established security, illegal immigration, or high epidemic risk factors. These factors might not necessarily pertain to the individual under consideration or their historical behaviour. Instead, they stem from collective observations involving specific third-country nationals and the associated personal data. These observations will inform the categorization of traits that could potentially trigger data matches under specific conditions.

The ETIAS Central Unit, functioning under the auspices of the *European Border and Coast Guard Agency* (FRONTEX), has been assigned the role of authenticating the personal information of applicants who activate an automated alert during the application procedure. In cases where the alert is substantiated or uncertainty remains, the typical course of action involves the National Unit of the traveller's intended destination initiating a manual evaluation of the application. Similarly, if the alert arises from data previously provided by a specific Member State, then the National Unit of that particular state would be responsible for further examination.[21] As seen in Fig. 1., this manual phase, encompassing legal recourse against the decision, falls within the domain of the domestic law of the National Unit responsible for making the decision (*manual process and decision-making*) and this way, the procedure leaves the sphere of direct administration.[22]

2.2. The decision (of the ETIAS National Unit) to decline a request

When the automated filtering system identifies a data match (in Fig. 1. referred to as a 'hit'), the ETIAS National Unit of the relevant Member State is obligated to decline the travel authorization under certain circumstances. This obligation arises if the match is linked to a prior alert for denied entry and residence stored in the SIS. Furthermore, if the travel document employed for the application is reported as lost, stolen, unlawfully taken, or invalidated within the SIS, the ETIAS National Unit is also required to reject the travel authorization request.[23] In all other cases,[24] the National Unit is obligated to evaluate the security or illegal immigration risk, retaining the discretion to determine whether to approve or reject a travel authorization. For this assessment,

[15] European Parliament and Council Regulation (EU) 2018/1240 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 [2018] OJ L 236/1, [hereinafter: Reg. (EU) 2018/1240] rec. (10).
[16] Reg. (EU) 2018/1240, rec 21; art 15.
[17] Reg. (EU) 2018/1240, art 33(1).
[18] Rocco Bellanova and Georgios Glouftsios, 'Formatting European security integration through database interoperability' (2022) 31 European Security 454.
[19] Reg (EU) 2018/1240, arts 34-35.
[20] Reg (EU) 2018/1240, art 33.
[21] Reg (EU) 2018/1240, rec (15), art 25; see also art 20.2.
[22] Reg (EU) 2018/1240, art 37(3).
[23] Reg (EU) 2018/1240, art 20 (a) (c) and art 26(3).
[24] Reg (EU) 2018/1240, art 20; art 26(4)-(5).

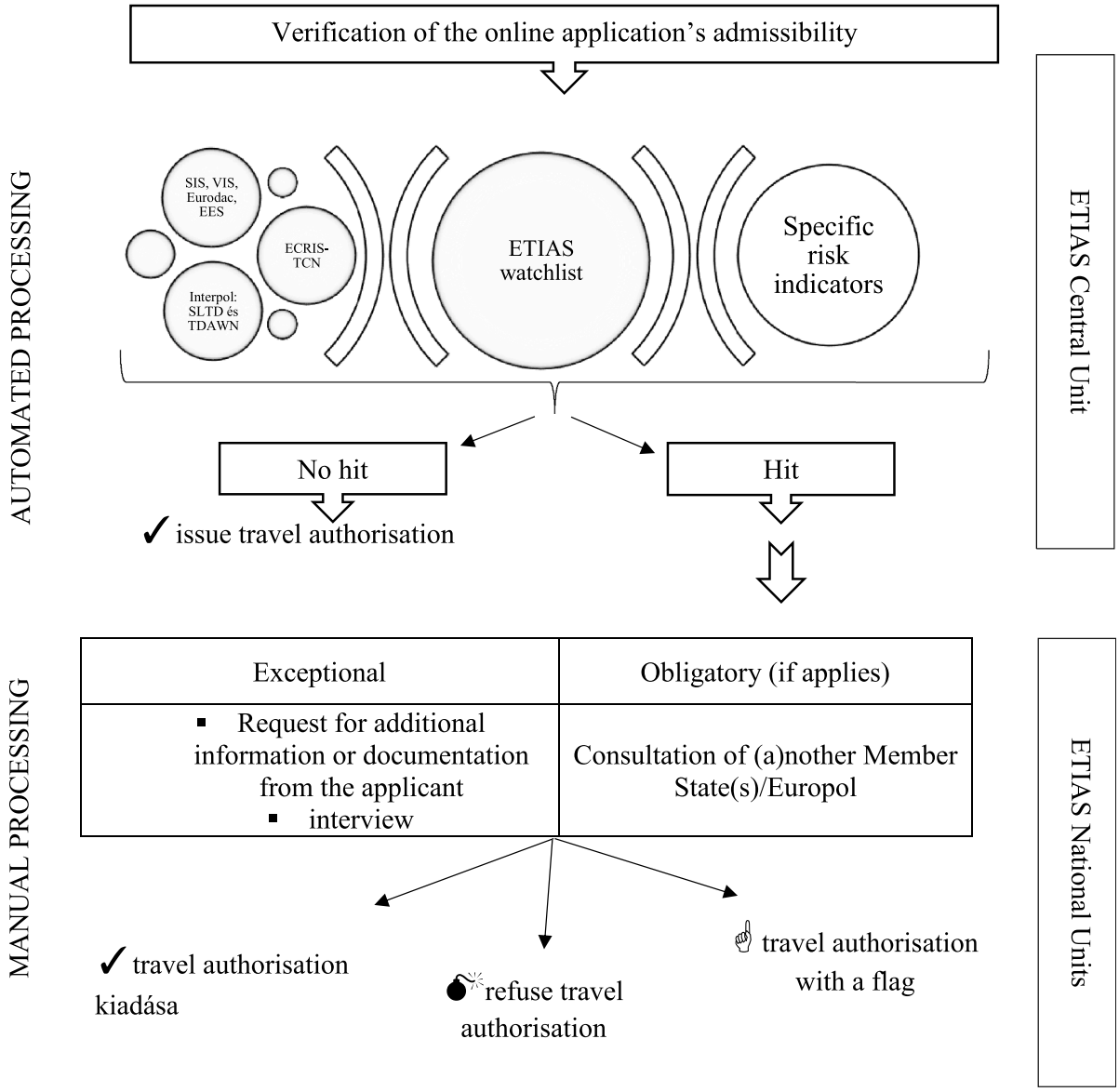

Fig. 1. Structure and functioning of ETIAS.

the National Unit holds the option to ask the applicant for supplementary documents[25] and, in unique cases, might even conduct an interview.[26] In respect of the general data protection directive (GDPR) that currently serves as the *lex generalis* to the procedure to the *lex specialis*, the ETIAS Regulation,[27] the ETIAS National Unit of the relevant Member State is prohibited from making an automatic decision solely based on a hit prompted by particular risk indicators. Instead, the National Unit must perform an individual evaluation of security risks, unlawful immigration risks, and elevated epidemic risks in all situations.[28] With this objective in mind, Member States possess the option, and at times an obligation, to engage in consultations with fellow Member States and Europol.[29] Nevertheless, the responsibility to establish their fundamental security interests and to enact suitable measures to safeguard both internal and external security rests solely with the Member States. Importantly, any determination reached by a Member State on this matter must adhere to EU legal principles and must not render EU law ineffective.[30] National measures undertaken to uphold public policy

[25] Reg (EU) 2018/1240, art 27(1)-(3). These options can be selected from a drop-down list, as provided in Annex II of Commission Delegated Decision (EU) 2022/1612 of 16 February 2022 specifying the content and format of the predetermined list of options to be used to request additional information or documentation pursuant to Article 27(3) of Regulation (EU) 2018/1240 of the European Parliament and of the Council [2022] OJ L 241/7.

[26] Reg (EU) 2018/1240, art 27(4)-(10).

[27] At present, in the absence of an administrative procedural code, the overarching data protection framework (GDPR and LED) establishes the fundamental procedural guidelines for managing personal data, which encompass automated decision-making as well. Maja Brkan, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' [2019] 27(2) International Journal of Law and Information Technology 91, 95-96.

[28] Reg (EU) 2018/1240, art 20(6).

[29] Reg (EU) 2018/1240, art 28-29.

[30] See, to that effect Case 742/19 *B. K. v Republika Slovenija (Ministrstvo za obrambo), Request for a preliminary ruling* [2021] EU:C:2021:597, para 40 and the case-law cited.

(*ordre public*) within a Member State must also be in harmony with this consideration.[31]

In summary, when a hit is identified, the automated decision-making procedure gives way to a manual process, necessitating human involvement to assess the situation. Consequently, the procedure encompasses two notably distinct phases leading up to the final decision.

When the decision is favourable, typically there is little cause for concern as it is expected to be issued within a matter of minutes after the application is submitted.[32] However, when the decision is adverse, it might trigger queries regarding the rationale behind it and the availability of legal remedies. It's important to mention that the forms for notifying decisions to refuse, annul, or revoke a travel authorization are automatically generated through the software utilized by the responsible ETIAS National Unit.[33]

Regarding the essence of the content, the software is designed to allow the officer to choose an appropriate form based on the type of decision (refusal, annulment, or revocation) and subsequently present a list requiring the selection of the relevant grounds for the decision. Notably, the field labelled 'statement of the relevant facts and additional reasoning underlying the decision' is obligatory within the form. Until this section is completed, the system prohibits the generation of the forms for final confirmation. Once this step is fulfilled, the software produces the decision in PDF format, which is then appended to the application file and transmitted to the applicant via email service.[34]

Regarding the rationale, it's crucial to note that the reasons for rejecting the ETIAS authorization can be divided into two distinct categories that dictate the justification for the decision. The first category (a) encompasses factual grounds, directly linked to the applicant's *personal conduct*, either in the past or during the manual processing of the ETIAS application. These reasons are supported by concrete evidence of specific issues. Within this category, the following reasons apply: (i) the travel document used by the applicant has been reported as lost, stolen, unlawfully taken, or invalidated in the Schengen Information System (SIS) by a Member State ;[35] (ii) there is an alert for refusal of entry and stay recorded in the SIS by a Member State ;[36] or the applicant did not cooperate in clarifying facts during the manual processing. It means that the applicant either failed to respond within the 10-day deadline to a request for additional information or documentation from the ETIAS National Unit[37] or failed to attend an interview as requested.[38] The second group of reasons (b) involves assumptions derived from profiling techniques based on patterns and indicators rather than direct evidence.

In instances of data correspondence within ETIAS, the primary responsibility for assessing the case rests with the Member State that entered or supplied the data leading to the hit. Consequently, in these situations, the decision-maker can provide a comprehensive overview of the decision's motives. These motives are directly linked to the individual's conduct and are primarily based on legal or authoritative determinations that resulted in their inclusion in a specific database, such as the ban on entry records in the SIS.[39]

When manual processing of an application is not prompted by data in the system previously provided by a Member State, it often implies that the individual's identification was caught by the filter due to profiling. In such cases, the Member State responsible for assessment is generally the Member State of the intended initial stay.[40] Regarding the reasoning behind such decisions, the decision-making National Unit faces the challenge of properly explaining the decision and aligning it with the established requirements for justifying administrative decisions. Simultaneously, the National Unit must strive to persuade the applicant of the factual and legal accuracy of the refusal. It is important to note that the remaining grounds for refusal offer considerable discretion to the National Units for assessing security risks,[41] illegal immigration risks,[42] high epidemic risks,[43] or *reasonable and serious doubts* about the provided data, statements, and/or supporting documents in the application.[44] Additionally, in the case of a travel authorization with limited territorial validity, entry is granted based on humanitarian considerations, national interest, or international obligations as defined by the national law of the Member State of the destination. If any of these specific circumstances are not met, it serves as a basis for refusal.[45]

If the Member State that engaged in collaboration during the manual processing presents an unfavourable opinion about the individual, it serves as an automatic basis for refusal by the reviewing National Unit. The collaborating Member State is free to assess the case and form an opinion based on its national procedures and practices. If the collaborating Member State opposes the presence of the TCN, the National Unit handling the proceeding shall reject the application unequivocally.[46]

The ETIAS regulation lacks substantial direction regarding the mandatory components of argumentative quality for decisions of refusal. However, there is no justification for disregarding the traditional principles of the rule of law during manual processing and decision-making. Adhering to the procedural rights of the applicant necessitates a lucid and transparent elucidation, encompassing the facts and context of the decision. This brings forth the question of how the proceeding National Unit interprets its responsibility to provide reasons.

In this context, it's prudent to explore the basis on which the decision is reached. As seen in Fig. 1, the two phases of the proceedings are not subordinated but are rather separated and consecutive. . First, the algorithmic phase that led to the hit necessitates an explanation elucidating the relationship between the applicant's provided data on the application form and the characteristics that contributed to their identification as a potential risk.[47] Second, the assessment of the National Unit shall be explained. The evaluation might be supported by the following supplementary elements: (i) consultation with other Member States leading to an opinion, that is assumed to be substantiated and binding on the proceeding National Unit; (ii) consultation with Europol, resulting in an opinion that isn't binding on the proceeding National Unit; (iii) supplementary documents furnished by the applicant, as required by the National Unit; (iv) the evidence resulting from an interview, if mandated by the National Unit. This comprehensive consideration underscores the multi-faceted nature of the decision-making process and the diverse sources of information and

[31] Joined Cases 368/20 and C-369/20, *NW v Landespolizeidirektion Steiermark (C-368/20), Bezirkshauptmannschaft Leibnitz (C-369/20)* [2022] ECLI:EU:C:2022:298. para 84.

[32] Reg (EU) 2018/1240, rec 21.

[33] The responsible Member State (and its designated authority as National Unit) for the manual processing depends on the nature of the hit and the data correspondence in the Central System as mentioned previously. See details: Reg (EU) 2018/1240, art 25.

[34] Based on Reg (EU) 2018/1240, art 38 (3), see the rules for establishing competence and jurisdiction: Commission Implementing Decision (EU) 2022/102 of 25 January 2022 laying down forms for refusal, annulment or revocation of a travel authorisation [2022] OJ L 17/59, art 1.

[35] Reg (EU) 2018/1240, art 37(1)(a).

[36] Reg (EU) 2018/1240, art 37(1)(e).

[37] Reg (EU) 2018/1240, art 37(1)(f).

[38] Reg (EU) 2018/1240, art 37(1)(g).

[39] Reg (EU) 2018/1240, art 25(1) (a)-(c).

[40] Reg (EU) 2018/1240, art 25(1).

[41] Reg (EU) 2018/1240, art 37(1)(b).

[42] Reg (EU) 2018/1240, art 37(1)(c).

[43] Reg (EU) 2018/1240, art 37(1)(d).

[44] Reliability of the data submitted; reliability of the statements made; the authenticity of the supporting documents submitted; veracity of the content of the supporting documents submitted. Reg (EU) 2018/1240, art 37(2).

[45] See, Reg (EU) 2018/1240, arts 44., esp. 44 2 and (6)(e).

[46] Reg (EU) 2018/1240, art 28 (7).

[47] Reg (EU) 2018/1240, art 20-21.

perspectives that contribute to the final determination.[48]

Following the requisites of sound reasoning, all pivotal aspects must be scrutinized to validate the legality of the decision and afford the applicant procedural safeguards. This latter includes the right to access their files while upholding the rightful concerns of confidentiality enshrined in the EU Charter's right to good administration.[49] The applicant should be apprised of the grounds for refusal, encompassing the factual basis, logical progression, and applied legal principles.

The administrative authority is obliged to provide adequate and specific justification for its decision, allowing the recipient to comprehend the reasons behind the individual measure that adversely affects them. This obligation arises from both the general principle of EU law and the principle of respecting the right to protection.[50] The comprehensibility of the reasons underlying a decision serves a dual purpose: firstly, a complete understanding of the case assists the party involved in deciding whether it is useful to appeal to the competent court; and secondly, it enables the court to review the legality of the relevant national decision.[51] In terms of the essence of the reasons underlying the decision, a fundamental criterion is whether the decision has a unique effect on the recipient. Assessing this does not limit itself to evaluating the abstract probability of the cited reasons but aims to determine whether these reasons – or at least one among them, which may be considered self-sufficient in supporting the decision – are well-founded.[52]

In simple terms, the National Unit of the Member State, responsible for making decisions and providing legal recourse, must justify its decisions. This includes cases involving concrete SIS alerts or specific risk indicators flagging individuals with potentially concerning personal backgrounds. This scenario engenders the query of precisely what the authority is required to validate within this context: whether it's solely the assessment conducted by the National Unit or also includes how the applicant was identified by the system filter, and whether the system outcomes can be considered factual.

3. The reasoning for the decision on the refusal

3.1. Reasoning as the heart of an authority decision

The reasoning behind an administrative authority's decision is considered a key element, if not the most crucial one, in establishing the legality of the process; its necessity has deep roots in history.[53] The rule of law necessitates the legality of the functioning of public administration. This begins with the exercise of power based on clear, accessible laws that allow foreseeability.[54] Legal certainty is a prerequisite to prevent arbitrary use of executive power, even in cases where broad discretion is permitted to choose the best interpretation of the law in a given situation. On the part of the administration, there exists a duty to provide reasons for decisions, while on the individual's side, the right to a reasoned decision is recognized as a fundamental right, as echoed in the EU Charter of Fundamental Rights.[55] The primary purpose of justification is to substantiate the decision both factually and legally, presenting it to supervisory organs and the addressee of the decision. It fulfils this purpose by explaining and arguing, covering all aspects of the decision-making process and procedure. Therefore, besides designating the body authorized to make the decision, the justification begins by establishing facts derived from legally relevant information, filtered from the vast sea of available data.

It presents the evidence accepted as the basis for the decision and provides all necessary information about the procedure for both the decision's addressee and the overseeing organ responsible for ensuring the administration's functioning and decision-making legality. Briefly, the reasoning is the evidence for the respect of fundamental laws and also all procedural guarantees.[56]

The quality of justification serves as evidence of adherence to procedural guarantees, which are vital for safeguarding individual rights and ensuring an effective remedy. To justify a decision effectively, the authority should avoid overly general, brief, and stereotypical statements, paying special attention to unique circumstances and tailoring justifications accordingly.[57] If the justification fails to establish legality, the decision is deemed illegal and unsuitable for substantive review.

The right to an effective legal remedy is infringed if the parties involved cannot examine the facts and documents on which decisions concerning them are based, hindering their ability to express their views.[58] Therefore, the importance of providing an effective legal remedy is underscored by the need for a thorough justification of authoritative rulings. Even if there is necessary human intervention by the ETIAS National Unit to render the final verdict on the traveller in all cases resulting in a hit, the decision-making process demands attention from the point of view of the reasoning behind a refusal. In general, the procedural deadlines are within 96 h after the application is submitted. During this time, the National Unit notifies the applicant about the decision: whether their travel authorization is approved, or denied or if additional information or documents are needed. If an interview is necessary, the decision must still be made within 48 h after the interview.[59] The decision-maker must provide a statement on the grounds of the decision. If the classical rules mentioned above are followed, this statement will necessarily draw connections with the nature of the case and the final decision, particularly when it is a negative one. This moment demands the utmost attention.

3.2. Automatisation of the risk assessment and the decision on travel authorisation: short process with long-term effects?

If there is no data match based upon the submitted application, the travel authorisation is an automated decision and constitutes a presumption-based decision indicating that there are *no factual indications or reasonable grounds* to consider that the presence of the TCN on the territory of the Member States poses security, illegal immigration or a high epidemic risk.[60] The question to explore is how the factual and

[48] Reg (EU) 2018/1240, art 26-29.

[49] EU Charter, art 41(2) al 2-3.

[50] Case 277/11 M. *M. v Minister for Justice, Equality and Law Reform and Others* [2012] EU:C:2012:744, para 88, case 249/13 *Khaled Boudjlida kontra Préfet des Pyrénées-Atlantiques* [2014] EU:C:2014:2431, para 38.

[51] Case 300/11 *ZZ és a Secretary of State for the Home Department* [2013] ECLI:EU:C:2013:363, para 53, Case 159/21 *Országos Idegenrendészeti Főigazgatóság and Others* [2022] ECLI:EU:C:2022:708, paras 48-49.

[52] Joint cases 584/10 P, 593/10 P and 595/10 P *European Commission contra Yassin Abdullah Kadi* [2013] ECLI:EU:C:2013:518, para 119.

[53] Giacinto Della Cananea, *Due Process of Law Beyond the State: Requirements of Administrative Procedure*(Oxford University Press, Oxford, 2016) 63.

[54] Venice Commission, Rule of Law Checklist (CDL-AD(2016)007, 2016) 11-12; CaseC-156/21 *Hungary v Parliament and Council* [2022] ECLI:EU:C:2022:97, 223-225; 230.

[55] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 [hereinafter: EU Charter] art. 41.2c.

[56] Case C-544/15 *Sahar Fahimian v Bundesrepublik Deutschland* [2017] ECLI:EU:C:2017:255, para 46; Cases C-379/08 and C-380/08 *ERG and Others* [2010] EU:C:2010:127, para 60-61; Case C-62/14 *Gauweiler and Others* [2015] EU:C:2015:400, para 69; Case C-269/90 *Technische Universität München* [1991] EU:C:1991:438, para 14; Case C-413/06 P *Bertelsmann and Sony Corporation of America v Impala* [2008] EU:C:2008:392, para 69.

[57] Decision on Code of Good Administrative Behaviour. [2011] OJ C 285/3 18.2.

[58] Case C-300/11, *ZZ. v. Secretary of State for the Home Department* [2013] ECLI:EU:C:2013:363, para 56.

[59] Reg (EU) 2018/1240, art 30; 32.

[60] Reg (EU) 2018/1240, art 3(5).

legal argumentation is presented in the decision as part of the reasoning – if there is a reasoning at all.

The issuance of the ETIAS permit does not occur in instances where there is a match within the databases. Instead, such situations result in the transfer of the case from the ETIAS Central Unit to the respective ETIAS National Unit. Consequently, human intervention is involved to individually examine whether the data match can be traced back to a reason justifying the decision to reject the travel authorization application.

There are arguments advocating for AI as the safest and most reliable decision-making tool.[61] As a safety feature, one might assume that the manual process filters out unreasonable cases, and most hits are merely warnings that can be easily overcome through the application of the necessity-proportionality test by the ETIAS National Unit, ultimately leading to the granting of the travel permit. However, as we delve into risk assessment, there are certain concerns to address. Firstly, the manual procedure is largely regulated by domestic rules, including the evaluation of risk factors. Given that it falls within the realm of national security assessments, such procedures involve the management of classified data (further explanation see below in chapter 4.3.). Secondly, due to the short deadlines that do not favour a detailed examination of the facts produced by the algorithms and the absence of harmonized material rules, Member States have significant discretion to assess risks that could endanger their national security. This makes it likely that the decision would lean towards a negative outcome rather than authorizing travel with a flag recommending a second-line check at the border crossing point or assuming the risk of issuing the travel permit for a potential risk holder.[62] So, the risk of having collateral damages is high.

When the data match is based on factual data alignment within the listed databases that hold factual proofs of behaviour based on judicial or authority procedures (*res iudicata*), and once personal identity is verified, it becomes considerably indisputable. Conversely, the match might also be the outcome of alignment with the watchlist or special risk indicators, possibly due to profiling.[63] Currently, the Commission does not provide further clarification on its regulation of specific technical matters,[64] whether it pertains to artificial intelligence or the utilization of a learning algorithm within the context of ETIAS. These terms have been used interchangeably thus far.[65] When it comes to automated decision-making, individuals have the entitlement to avoid being subjected to decisions that exclusively result from automated processing, encompassing profiling. Such decisions can have legal consequences or similarly noteworthy impacts on the individual. Nonetheless, it is necessary to examine more closely the factual basis and rationale behind such decisions as prerequisites for establishing an effective avenue for legal recourse. As *Bayamlıoglu* raises, automated decision-making systems "*may also be seen as techno-regulatory assemblages, which select and reinforce certain values at the expense of others*",[66] and as it is known, GDPR ensures certain rights but an *explicit right for an explanation* for individual automated decisions is not provided. Here comes the challenge that engenders here, in this phase of the procedure but becomes tangible when the ETIAS National Unit issues the refusal decision or even later. First, it is related to gaining information on the refusal and the reasoning behind the decision as a matter of individual interests, and it is discussed below. The second aspect can also be interpreted in a wider context, *pro futuro*.

In principle, a previous refusal of a travel authorisation the refusal (or withdrawal or annulment of travel authorisation) shall not lead to an automatic refusal of a new application and a new application shall be assessed based on all the available information.[67] However, the data given and also the negative decision will form a part of this 'available information', and like all data once entering the system, will contribute to, inter alia, the statistics that lead to the regularly updated specific risk indicators. Thus, any sort of data of a person whose travel permit request was denied will certainly contribute to those indicators that motivate the next update on the filtering system. Control over personal data seems given by the right to data retention or erasure for instance,[68] although on the other hand, in practice it seems unpracticable. In fact, not much is known about how the algorithm will work beyond those cases when the *res iudicata* nature of database information results in a hit, although as *Eklund* highlights, these technical specifications of algorithms will function as law. They will have implications on decision-making even if they are not law and do not ensure clarity and foreseeability.[69]The heart of the whole system and data handling centres around the provided personal data set. Subsequently, insights garnered from case statistics will manifest in the form of special risk indicators.[70] In terms of data accuracy and lawful recording within the ETIAS system, applicants possess the right to challenge, access, rectify, erase, and restrict the processing of their personal data stored in ETIAS. If the ETIAS Central Unit or the relevant ETIAS National Unit of the Member State responsible for the application disagrees with the claim, they must promptly make an administrative decision that elucidates in writing why they are unwilling to correct or erase the data. Moreover, applicants have the right to seek legal recourse and have their data processing supervised by independent public authorities.[71] In this context, it's essential to consider the balance of interests. This involves aligning the interoperability of multiple databases, including those containing ETIAS watchlist data and specific risk indicators, with the GDPR's principle of limiting purposes and the *right to be forgotten*.[72] While exceptions rooted in substantial public interests supported by security rationales exist, concerns have been voiced about the blending of law enforcement and migration objectives in data processing, as highlighted by *Quintel*.[73] As the database incorporates additional functionalities, the distinction between border control and security goals becomes muddled, making it challenging to clearly define processing purposes. The roles of entities engaged in ETIAS data processing are often ambiguous, which further complicates matters.[74] Furthermore, the practical implementation of the right to be forgotten and its implications for the use of special risk

[61] Yulia Razmetaeva and Natalia Satokhina, 'AI-based Decisions and Disappearence of Law' (2022) 16(2) Masaryk University Journal of Law and Technology 245.

[62] Reg (EU) 2018/1240, art 36. 2-3.

[63] GDPR, art 4(4) on the definition of profiling *cf* Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Hildebrandt, M and Gutwirth, S, *Profiling the European Citizen Cross-Disciplinary Perspectives*, 17-19 (Springer, Dordrecht 2008).

[64] Commission Delegated Regulation (EU) 2021/1253 of 21 April 2021 amending Delegated Regulation (EU) 2017/565 as regards the integration of sustainability factors, risks and preferences into certain organisational requirements and operating conditions for investment firms (Text with EEA relevance) [2021] OJ L 277/1, arts 3-6.

[65] Costica Dumbrava, Artificial intelligence at EU borders. Overview of applications and key issues (European Parliamentary Research Service, PE 690.706, July 2021), Charly Derave, Nathan Genicot and Nina Hetmansk, 'The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System' (2022) 13(3) European Journal of Risk Regulation 389, 394.

[66] Emre Bayamlıoglu, 'The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation"' (2022) 16 Regulation & Governance 1058, 1063.

[67] Reg (EU) 2018/1240, art. 37.4.

[68] Reg (EU) 2018/1240, art. 54-55.

[69] Eklund (n7) 265.

[70] Reg (EU) 2018/1240, art 33.1, 2 b), c).

[71] Reg (EU) 2018/1240, rec 57, art 64; GDPR, arts 17 to 20.

[72] GDPR, art 5(1) (b) and 17.

[73] GDPR, art 6(3); rec 50-53.; arts 17 and 23.1.c) *cf* art 89. see also Rebeca Ferrero Guillén, 'The 'Right to Be Forgotten' Does Not Apply to Facts of Public Interest' (2023) 72(2) GRUR International 193.

[74] Teresa Quintel, *Data Protection, Migration and Border Control. The GDPR, the Law Enforcement Directive and Beyond* 39 (Hart, Oxford 2022).

indicators are not yet definitively established. Scholars like *Villaronga, Kieseberg*, and *Li* underscore the difficulty of attaining the legal objectives of the right to be forgotten within artificial intelligence contexts, necessitating further clarification.[75] Concurrently, each application file is stored in the ETIAS Central System either for the travel authorization's validity period or for five years from the last decision to deny, annul, or revoke the authorization. Under specific circumstances, this duration might be extended by an additional three years.[76] A prior travel authorization refusal does not automatically result in a new application denial,[77] and applicants can retract their consent at any time, causing their application file to be automatically removed from the ETIAS Central System,[78] however, data linked to an individual whose entry was initially denied but was subsequently erased might impact the profiling of others. The *principle of fairness* mandates that the processing of personal information should be carried out while respecting the data subject's interests and anticipations. If there are suspicions or claims that an algorithmic model yields unjust or discriminatory outcomes, the Data Protection Authority holds the authority to investigate for the sake of ensuring fairness. This could encompass reviewing documentation for data selection, assessing algorithm development, and scrutinizing proper testing protocols before implementation.[79]

On the other hand, GDPR acknowledges specific limitations on individual rights for greater, namely public (law enforcement) purposes,[80] and many aspects of data management and processing primarily fall within the scope of the law enforcement directive (LED). Ensuring the smooth flow of personal data between competent authorities to mitigate and prevent threats to public security within the European Union is vital, all while upholding a high level of personal data protection.[81]

Additionally, the entity responsible for data control is obligated to implement suitable measures for safeguarding the data subject's rights, freedoms, and lawful interests. This includes their right to express opinions and contest decisions.[82] The *right to contest*, grounded in the concept of an effective legal recourse, encompasses the entitlement to be informed about the factors contributing to the decision. This encompasses the factual context and the corroborating evidence. Consequently, the right to contest necessitates the provision of supplementary information or pertinent details that are essential for a comprehensive understanding of the profiling process. This entails elucidating how the personal data furnished was employed to formulate a profile indicating a potential risk. Such an explanation surpasses mere data access or furnishing technical insights into AI operations. When viewed from the perspective of decision rationale prerequisites, this entails offering an explanation that establishes a clear link between facts and legal provisions.

It should be acknowledged that due to its nature as an AI system, the decision-making process within ETIAS carries a significant risk, as it has the potential to adversely affect both individuals' safety and their fundamental rights, as safeguarded by the EU Charter of Fundamental Rights.[83] Derived from the *principle of transparency*,[84] it is imperative that information regarding the utilization of personal data be easily accessible and presented in clear language. Nevertheless, the complexity introduced by advanced technology and opaque processes makes it challenging to elucidate how information is correlated and assigned weight within a given procedure. While the *right to access information* empowers individuals to request details about the personal data employed in decision-making, it does not inherently encompass the right to an explanation for said decisions.[85]

However, a semblance of the *right to explanation* is indicated in a recital of the GDPR, which underscores the necessity for implementing safeguards to protect data subjects' rights. This includes "*the right to express their point of view, obtain an explanation for the decision made following such an assessment, and challenge the decision*."[86] These safeguards are required to provide specific insights into how data was evaluated and considered, coupled with the entitlement to human intervention and the capacity to contest the decision.

3.3. The evaluation conducted by the National Unit

Since the refusal decision is legally attributed to the ETIAS National Unit, the responsibility to provide explanations rests with the relevant national authority overseeing the evaluation process. Despite the simplicity of the form, there is a specific section requiring textual evaluation. Thus, before saving and submitting the work, a rationale must be written.[87] If the National Unit is tasked with assessing pre-established facts and only verifies data for confirmation, it becomes crucial to provide a comprehensive explanation. Likewise, if a presumption arises from profiling based on case particulars, it logically requires elucidating why or how this presumption was substantiated by the National Unit. The question, therefore, is what tools national law provides to authorities for assessing the perceived or actual security risks associated with the TCN especially when the initial phase produces a risky profile based on specific risk indicators. It is the duty of the proceeding authority (the ETIAS National Unit) to justify a refusal decision, often based on such presumptions. The Court of Justice of the European Union (CJEU) recognizes the importance of referencing prior individual acts that outline the grounds for subsequent individual decisions issued by the same institution, particularly if they pertain to the same subject matter.[88] The *right to an explanation* is not explicitly spelt out in the GDPR itself. While the regulation does necessitate the provision of *meaningful information* about the rationale and significance of machine learning systems, it doesn't impose a specific degree of transparency concerning individual decisions. Despite this, the data controller remains accountable for supplying adequate information to enable the data subject to exercise their rights. This implies that the decision must be explicated in a manner understandable to the data subject, and they

[75] Eduard Fosch Villaronga, Peter Kieseberg and Tiffany Li, 'Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten' (2018) 34 Computer Law & Security Review 304.
[76] Reg (EU) 2018/1240, art 54.
[77] Reg (EU) 2018/1240, art 37.4.
[78] Reg (EU) 2018/1240, arts 54-55 *cf* the right to be forgotten in GDPR, rec 65-66 and art 17.
[79] Artificial intelligence and privacy. Datatilsynet [The Norwegian Data Protection Authority, January 2018] 19. https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf accessed 20 August 2023 [hereinafter: Norwegian AI Report] 16.
[80] GDPR, art 23.
[81] European Parliament and Council Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89 [hereinafter: LED] rec 4.
[82] GDPR, art 22.
[83] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts COM(2021) 206 final [2021] rec 39.
[84] GDPR, arts 12, 13, and 14.
[85] Ibid 22.
[86] GDPR, Rec (71).
[87] Reg (EU) 2018/1240, art 1.5.
[88] Case 16/65 *Firma G. Schwarze v Einfuhr - Und Vorratsstelle Fuer Getreide und Futtermittel, Frankfurt Am Main* [1965] ECLI:EU:C:1965:117, 888, see also e.g. Case 119/97 P *Union française de l'express (Ufex), formerly Syndicat français de l'express international (SFEI), DHL International and Service CRIE v Commission of the European Communities and May Courier* [1999] ECLI:EU:C:1999:116, para 57.

must be informed about the avenues for appeal or request human intervention.[89] The GDPR mandates that the controller furnish meaningful details about the logic employed, not necessarily an intricate exposition of the algorithms employed. However, the provided information must be sufficiently comprehensive for the data subject to grasp the grounds behind the decision.[90] Consequently, the right to receive 'meaningful information about the logic involved' in automated decisions can be viewed as a manifestation of the right to explanation, potentially leading to inquiries about the 'right to know why'.[91] This necessity is not fulfilled by general information accessible to the public on the dedicated website concerning the processing of personal data, as it doesn't provide meaningful insights in individual cases.[92] Additionally, while the refusal decision template includes information about available data protection avenues, this implies the need for information about the inherent procedural steps and the forum involved in making informed decisions regarding seeking justice.

Conversely, the ETIAS regulation allows for recording the outcomes of supplementary evidentiary procedural steps as an extension of the application file, and this supplementary information could be treated as a complementary aspect of the decision-making process. When the National Unit records the opinion of the consulted Member State in the application file, this practice could take precedence.[93] Moreover, in instances where Europol issues a negative opinion, but the responsible ETIAS National Unit decides to grant the travel authorization, it is required to justify its decision and document this rationale within the application file.[94] In rare cases involving interviews, the reason for requesting the interview must be documented in the application file. Subsequently, the interviewer's opinion, along with the justifications for their recommendations and the addressed elements, is recorded and included in a form within the application file on the same day as the interview.[95] These additional pieces of evidence contribute to the case documentation attached to the application file, ensuring accessibility for the applicant.[96]

However, the specific content of these opinions, as well as the reasoning behind the decisions made by the National Unit, fall outside the scope of the ETIAS regulation. The assessment process operates under the ETIAS regulation as the general framework for the procedure, while the evaluation of the individual is guided by the national law as the specialized legal framework. This dynamic underscore the challenges connected to classified information grounded in national security concerns. Member States possess the flexibility to deviate from the general rule of granting individuals access to files, especially when revealing information or its sources could potentially jeopardize national security or the security of the sources involved.[97] Member States possess an internationally recognized discretion to assess what constitutes a threat to their national security and how it should be addressed as threats to national security may vary in character and be unanticipated or difficult to define in advance.[98] When evaluating information related to national security, public safety, and public order, the primary criterion is legal compliance with the procedure. This means that the national laws governing the process should meet essential quality standards, ensuring accessibility, clarity, and predictability.[99] Hence, the answer to the question of what can serve as the basis for identifying risk is simply anything that the State deems pertinent in each situation and context. As for the EU acquis, it is also a delicate matter to define what may be considered as such. The legal practice already has weak points for TCNs when their potential threat to national security or public order is assessed due to the lack of access to files of classified documents,[100] even without the prior algorithmic phase of the procedure resulting in a certain profile and the reasons for it. Meanwhile, such circumstances that resulted from the profile are crucial first, to be able to contest the result and, second to practice control over the personal data. LED recognizes the rights of Member States to enact legislative measures that might delay, restrict, or omit the provision of information to data subjects, as long as these measures are deemed necessary and proportionate within a democratic society. This empowers the National Unit to balance the fundamental rights and legitimate interests of the individual against the foundational interests of the State like avoiding obstructions to official or legal inquiries, investigations, or procedures, safeguarding public security, and protecting national security. This involves broad discretion in determining how these factors should be weighed.[101] The same reasons can support limitations to the right of access as well. This weighing process also reinforces the objective of collecting and processing personal (criminal) data for preventative functions, particularly concerning national security concerns.[102] *Vadász and Ződi's* observations, in alignment with the WP 29 guidance, underscore that the exceptions' scope is so extensive that the Member States can effectively nullify the right of access, rendering human intervention ineffective as a means of balancing the risks of profiling.[103] Simultaneously, *Vadász and*

[89] Ibid 21-22, see Reg (EU) 2018/1240, arts 1-2.

[90] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (wp251rev.01, 6 February 2018) 24 - 25 https://ec.europa.eu/newsroom/article29/items/612053 accessed 20 August 2023 [hereinafter: Article 29 WP Guideline].

[91] Andrew D. Selbst and Julia Powles 'Meaningful information and the right to explanation' (2017) 7(4) International Data Privacy Law 233, 242.

[92] Reg (EU) 2018/1240, arts 16 and 71, GDPR, art 15 (1) (h).

[93] Reg (EU) 2018/1240, art 28(3).

[94] Reg (EU) 2018/1240, art 29(8).

[95] Reg (EU) 2018/1240, art 27(4) and (8).

[96] EU Charter, art 8(2).

[97] Case 159/21 (n 44) paras 37-38.

[98] *C.G. and others v. Bulgaria* App no 1365/07 (ECtHR, 24 July 2008) 40; Case C-380/18 *Staatssecretaris van Justitie en Veiligheid v E.P* [2019] ECLI:EU:C:2019:1071, 37. Erzsébet Csatlós, ' National Security-Related Expulsion Cases during the Pandemic in Hungary: Secret Revealed?' (2023) 43(2) Acta Iuris Stetinensis 32; Václav Stehlík, 'Discretion of Member States vis-à-vis Public Security: Unveiling the Labyrinth of EU Migration Rules' (2017) 17(2) International and Comparative Law Review 137-138.

[99] Didier Bigo and others, National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges. Study for the LIBE Committee, 45-46 (Directorate General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs Justice, PE 509.991. 2014) https://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf accessed 20 August 2023.

[100] Case C-159/21 *GM v Országos Idegenrendészeti Főigazgatóság, Alkotmányvédelmi Hivatal, Terrorelhárítási Központ* [2022] ECLI:EU:C:2022:708, 43-44; 53.

[101] LED, art 13(3) (a), (c), (d).

[102] LED, art 15(1) (a), (c), (d).

[103] Pál Vadász and Zsolt Ződi, 'The Accountability of Intelligence and Law Enforcement Agencies in Information Search Activities' in International Conference on Electronic Participation [ePart 2021] 9 https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/20324/The_accountability_of_intelligence_and_law_enforcement_agencies_in_information_search_activities.pdf?sequence=4&isAllowed=y accessed 20 August 2023 *cf* Article 29 WP Guideline (n 97) 34-35.

Ződi highlight a restrictive interpretation of necessity and proportionality in line with the ECtHR practice.[104]

Addressing the procedural safeguards that are designed to establish the boundaries of legality for the decision-making process in the context of the ETIAS permit, it is the responsibility of the Member States to develop practical procedures that safeguard rights within their domestic legal frameworks, in alignment with the principle of procedural autonomy. These procedures must offer a level of protection that is at least as advantageous as those applied to analogous domestic scenarios (*principle of equivalence*). Additionally, these procedures should not create circumstances where the exercise of rights granted by EU law becomes unduly challenging or impractical (*principle of effectiveness*).[105]

To challenge a decision where the facts are possibly based on presumptions of a profile is difficult, if not possible. Firstly, data management and AI functioning that results from the profile is beyond the Member State's jurisdiction. It shall be a subject of legal remedy but based on a proper explanation of how to access justice in this field. Secondly, the profile is the reason why the case gets to the jurisdiction of the National Unit. There is no uniform definition of national security, public security, or public order in EU law due, inter alia, to the already mentioned reasons. For EU citizens, a measure (expulsion) taken in the name of public security must be based exclusively on the personal conduct of the individual concerned and that conduct must represent a 'genuine, present and sufficiently serious threat' to that fundamental interest of society,'[106] but in the case of a TCN, the admission may be refused when only 'potential' threat to public security is resulted from the assessment of the facts when the foreseeable conduct of the applicant is predicted. Such a process must be based inter alia on extensive knowledge of his or her country of residence and the analysis of various documents and the applicant's statements,[107] but the competent national authorities still enjoy wide discretion when assessing the relevant facts to decide upon the existence of a potential threat.[108] Contesting the circumstances deliberated upon is thus challenging, especially if access to documents, including reasons, is difficult, regardless of formal access to the law. Recent legal precedents demonstrate how formal provisions outlining legal remedies can create the appearance of procedural safeguards. However, in practice, the effectiveness of these safeguards can be compromised, particularly in cases involving national security concerns. Invoking national security considerations is always sensitive, and the complexities of automated decision-making, including profiling, raise more questions than solutions. Although human intervention in manual processing may introduce oversight, it might not adequately address the unintended consequences of profiling. When evaluated in terms of access to documents, understanding decision rationales, and viable legal remedies, this approach may still fall short of expectations.[109]

4. Conclusion

AI might be argued as the safest and most reliable decision-making tool, but the interplay of the ETIAS screening process, data protection regulations, and national security concerns presents an intricate scenario that seems to challenge procedural rights. The rights to access files and to receive explanations for decisions stand as essential components of effective legal remedy, while the imperative to safeguard national security remains a legitimate interest for both the individual Member States and the collective security union. This dynamic resembles a sort of procedural Bermuda triangle, where rights and interests intersect.

When examining the fundamental requisites for authority decisions within the digital realm, a pivotal inquiry emerges: does the simplification of the process through IT tools and artificial intelligence still correspond to the EU values, especially procedural rights? In the context of balancing national security considerations underpinning classification with the right to receive a reasoned decision, the latter seems to have taken precedence. Scrutinizing the refusal decision entails delving into factors influencing its content and the legal provisions contributing to the core of the National Unit's obligation to provide reasons for its decision. This justification draws from two distinct yet interconnected elements: the factual and the legal basis. Of these, the section focusing on facts involves the necessity to disclose profiling information. Even though an explicit explanation right isn't explicitly granted, substantial information must be furnished to empower the individual to contest the decision. Consequently, the methodology of profiling should be an integral part of substantiating the decision, as the typical general descriptions of system functioning fail to clarify specific cases.

Conversely, fact-clarifying actions that arise in connection with manual procedural steps can be attributed to the processing authority. Following the procedural stipulations of the ETIAS Regulation, the processing authority must also upload opinions stemming from consultations and interviews (if conducted) to the application file. While these opinions become part of the personal documentation linked to the application file, it's important to recognize that Member States wield substantial discretionary power in evaluating whether the presence of third-country nationals poses a threat to national security and public order. They also possess the authority to delay, limit, or omit information provided to data subjects or to restrict data access, all in the interest of safeguarding public safety or national security. This latitude could potentially render the decision not amenable to review.

While there is considerable discretion based on the array of pertinent circumstances surrounding an individual's situation, it is still evident from legal precedent that the authorities involved must rely on robust reasoning, substantial factual foundations, and respect for essential procedural guarantees. These guarantees encompass a meticulous and unbiased examination of all relevant aspects by these authorities, coupled with the obligation to adequately justify the decision. Furthermore, the national court can scrutinize the interplay of factual and legal elements forming the basis of discretionary actions. From this perspective, the substance of the National Unit's duty to provide reasons can be ascertained, even when the decision-making process predominantly takes place within the digital realm.

In summary, it can be asserted that while algorithms have the potential to shape the evolution of the legal status of TCNs, they cannot

[104] Vadász and Ződi (n 110) 10.

[105] Considering the significance of access to documents, for instance, Case 430/19 *SC C.F. SRL v A.J.F.P.M., D.G.R.F.P.C* [2020] ECLI:EU:C:2020:429, paras 34-37.

[106] Case C-348/09 *P.I. v Oberbürgermeisterin der Stadt Remscheid* [2012] ECLI:EU:C:2012:300, para 30; Case C-165/14 *Alfredo Rendón Marín v Administración del Estado* [2016], EU:C:2016:675, para 84; Case C-304/14, *Secretary of State for the Home Department v. CS* [2016] EU:C:2016:674, para 40.

[107] Case C-84/12 *Rahmanian Koushkaki v Bundesrepublik Deutschland* [2013] EU:C:2013:862, para 56 and 57.

[108] Case C-544/15 Sahar Fahimian v Bundesrepublik Deutschland [2017] ECLI:EU:C:2017:255, para 40.

[109] See, Case 159/21 (n 44) para 94 1-2, also, Gruša Matevžič and others, 'The Right to Know: Comparative Report on Access to Classified Data in National Security Immigration Cases in Cyprus, Hungary and Poland' (Hungarian Helsinki Committee, Budapest 2021).

definitively determine it on their own. Thus, the human element retains ultimate authority in decision-making processes. However, inherent weaknesses within the decision-making system can introduce uncertainties, impacting not only the legal status and destinies of TCNs but also other stakeholders, potentially contributing to a sense of insecurity while pursuing the illusion of Europe's security. The ETIAS was designed to contribute to the establishment of a security union by serving as a zero-level filter on immigration for security reasons through the newest achievements of technology. However, it contains elements that instead create an 'insecurity union' regarding procedural rights and thus challenge the area of freedom, security, and *justice*.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

The research was supported by the ICT and Societal Challenges Competence Centre of the Humanities and Social Sciences Cluster of the Centre of Excellence for Interdisciplinary Research, Development and Innovation of the University of Szeged. The author is a member of the Artificial Intelligence and Legal Order research group.