Hungarian Journal of Legal Studies 66 (2025) 2, 97–112
DOI: 10.1556/2052.2025.00503

1828
AKADÉMIAI KIADÓ

Algorithmic immigration control? The ETIAS between technological benefits and fundamental rights considerations

ÁGOSTON MOHAY*

Faculty of Law, University of Pécs, Hungary

ORIGINAL RESEARCH PAPER

Received: October 22, 2023 • Accepted: July 4, 2025
Published online: December 17, 2025

ABSTRACT

The European Union (EU) aims to become a trendsetter in regulating the use of artificial intelligence (AI), especially in fields that are considered high risk – such as, for instance, migration control. The EU is already using various advanced technologies in its migration and asylum policy, and will expand its toolbox via the European Travel Information and Authorization System, requiring visa-exempt individuals traveling to the EU to register and provide personal data. The data will be filtered automatically, based on various specific risk indicators. The fundamental rights-compliant nature of such automated filtering needs to be assured, having regard to the EU Charter of Fundamental Rights and the various data protection regimes enacted by the EU – as well as the jurisprudence of the Court of Justice of the European Union. The paper analyses the algorithmic decision-making process of the ETIAS in light of all of the above, and concludes that the system is lacking certain safeguards, possibly imperiling not only the right to privacy and data protection but the right to an effective judicial remedy as well.

KEYWORDS

ETIAS, border control, artificial intelligence, automated decision-making, fundamental rights, data protection, privacy, PNR

* Corresponding author. E-mail: mohay.agoston@ajk.pte.hu

1. INTRODUCTORY THOUGHTS

Migration and asylum issues have had a steady place on the agenda of the European Union, especially since the 2015 crisis. The EU has been struggling to thoroughly reform these policy fields for quite some time,[1] even though recent emergencies such as the conflict in Ukraine have underlined their significance. In the meantime, new technologies including (but certainly not limited to[2]) artificial intelligence continue to develop and enjoy increased prominence in the EU. Both phenomena require a regulatory response by the EU if it intends to manage them well – and the EU has indeed introduced relevant legislative measures to reform migration and asylum law[3] as well as to regulate the use of artificial intelligence.[4]

The two abovementioned fields also intersect. The EU has been weaving technological tools into the tapestry of its migration and asylum policies in various ways. The 'smart borders' concept was initially proposed in 2013,[5] involving a centralized Entry/Exit System (EES) for third-country nationals crossing EU external borders for a short stay at its core.[6] The EU uses technology to collect and share border surveillance information gathered from satellites and other surveillance tools.[7] More generally, the various electronic justice and home affairs

[1]This has been an ongoing issue at least since the 2015 migration and asylum crisis. EU legislators (and, notably, the Member States represented in the Council) have been unable to overcome a negotiation deadlock since 2016. To address this conundrum, the Commission proposed a New Pact on Migration and Asylum in 2020. Commission, 'Communication from the Commission on a New Pact on Migration and Asylum' COM (2020) 609 final. Following lengthy and often heated political debates, the legislative elements of the Pact were fully adopted by both the European Parliament and the Council by 14 May 2024. Most measures in the reform package will become applicable two years after entry into force, i.e., in 2026.

[2]One can point, for example, to the Digital Services Act (DSA) and the Digital Markets Act (DMA). For an overview and analysis, see Hohmann and Kis Kelemen (2023).

[3]For the state of play of the proposals contained within the abovementioned New Pact, see: Link1.

[4]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L1689/1. (Hereinafter: AI Regulation.) The intent to regulate and harness modern technology and AI was already present in the EU's relevant (and numerous) strategic documents; for an overview of the latter, see e.g. Ritó (2021).

[5]The relevant Commission proposal package consisted of setting up an Entry-Exit System and modifying the Schengen Borders Code. Commission, 'Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security' COM (2016) 205 final.

[6]Admittedly, the EES Act took considerable time to adopt. Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 [2017] OJ L327/20.

[7]This takes place predominantly via EUROSUR. The original Regulation (EU) 1052/2013 of the European Parliament and of the Council establishing the European Border Surveillance System [2013] OJ 2013 L295/11 has been repealed by Regulation (EU) 2019/1896 of the European Parliament and of the Council on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 [2019] OJ L 295/1 and operates integrated into the EBCG framework.

databases managed by eu-LISA should be mentioned.[8] For understandable reasons, the interoperability of various security-related systems has also been emphasized[9] and regulated.[10] In terms of border control, migration and security, the EU is either already using or considering using AI tools in four ways: biometric identification, emotion detection, migration monitoring and forecasting, and algorithmic risk assessment.[11] This paper's analysis concerns the latter.

With the availability of significant computational capacity and big data, it is not surprising that the EU itself is exhibiting signs of 'techno-solutionism'.[12] A new instrument of EU border and migration control, and one that relies heavily on technology, is the European Travel Information and Authorisation System (ETIAS).[13] The ETIAS is actually not *that* new, as its underlying regulation was adopted in 2018. It was proposed by the Commission as far back as 2016 as part of the 'Bratislava Declaration and Roadmap' in response to various migration-related terrorist incidents that had occurred in the EU.[14] The implementation of the ETIAS in practice has, however, been considerably and repeatedly delayed for various reasons, including technical issues and the COVID-19 pandemic. The system will foreseeably finally become operational and applicable in practice in the last quarter of 2026.[15]

As a new form of travel authorization, the ETIAS will facilitate the screening of individuals who do *not* need a visa to travel to the EU. The electronic ETIAS system will require visa-exempt individuals to submit themselves to an automated application process, which entails the automatic processing of their personal data – which may result in 'hits' (i.e. positive matches).[16] Applications that produce hits will be manually verified by the ETIAS Central Unit and processed by the ETIAS National Units, with various options depending on the reason for the hit.[17] ETIAS will rely on screening rules – defined by the ETIAS Regulation as 'an algorithm enabling profiling' – that rely on specific risk indicators established by the ETIAS Central Unit (operating

[8]Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 [2018] OJ L295/99.

[9]Commission, 'Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security' COM (2016) 205 final.

[10]Regulation (EU) 2019/817 establishing a framework for interoperability between EU information systems (borders and visa); Regulation (EU) 2019/818 establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration). On the evolution and relevance of this concept, see e.g. Duić and Rošić (2022).

[11]Dombrava (2021).

[12]Vavoula (2021) 457.

[13]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 [2018] OJ L236/1 (ETIAS Regulation).

[14]The Bratislava Declaration and Roadmap was adopted by the EU's leading political body, the European Council, on 16 September 2016. Link2. The ETIAS is *grosso modo* similar to the Electronic System for Travel Authorization used by the USA or the Electronic Travel Authorization applied by Canada.

[15]Link3.

[16]ETIAS Regulation, preamble recitals (23)–(25) and art 20.

[17]ETIAS Regulation, art 26.

within FRONTEX, the European Border and Coast Guard Agency[18]) relating to security, illegal immigration or high epidemic-related risks.[19] Hits regarding these risk indicators may result in a refusal of travel authorization. Positive decisions by the algorithm do not require human involvement; thus, the system of decision-making may be considered automated regarding positive decisions and semi-automated in cases of 'hits'.[20]

In any case, the ETIAS will involve a form of algorithmic profiling and decision-making that utilizes artificial intelligence in some form. This raises potential fundamental rights issues that we will consider below.

2. ALGORITHMIC DECISION-MAKING AND FUNDAMENTAL RIGHTS

Algorithmic decision-making involves a number of broader and more specific fundamental rights challenges. First, as summarized by Gerards, algorithms are human constructs (which implies that they may have human flaws embedded in their functioning); they are often non-neutral (due to the biases and stereotypes present in the datasets that are used), and they are also non-transparent (i.e. the complexity of many algorithms, especially ones that use deep learning or machine learning are very difficult to understand, even for 'insiders' – thus creating what has been termed the 'black box effect').[21] These general characteristics can impact equal treatment, non-discrimination, and the right to a fair trial.[22] As has been shown, the use of machine learning systems has resulted more than once in discriminatory outcomes due to the use of inappropriate data for 'training' the systems.[23]

The applicability of the EU Charter of Fundamental Rights (hereinafter referred to as the Charter or CFR) in the context of ETIAS is unquestionable: in the course of applying ETIAS, EU institutions and relevant national authorities are both applying EU law.[24]

As for the relevant rights, in a general sense, equality and non-discrimination are enshrined in Articles 20–21 of the EU Charter. More specifically, the right to respect for private and family life (Article 7 of the CFR) and the right to protection of personal data (Article 8 of the CFR) are relevant. Furthermore, regarding the right to protection of personal data, at the level of secondary EU law, the General Data Protection Regulation (hereinafter: GDPR) contains safeguards vis-à-vis algorithmic decision-making.[25] As the GDPR is not applicable to the processing of

[18]ETIAS Regulation, art 7 (1).

[19]ETIAS Regulation, art 33 (1).

[20]Musco Eklund (2022).

[21]Gerards (2019) 205.

[22]Gerards (2019) 206.

[23]Cf. Reichel and Molnár (2023) 159–61; Mezei and Bán-Forgács (2022) 74–75.

[24]Cf. Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 51.

[25]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 [2016] OJ L119/1 (GDPR), art 22.

personal data by authorities for the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and prevention of threats to public security,[26] the EU further has a specific directive applicable to data protection related to criminal offences or the execution of criminal penalties; this directive contains an essentially identical sister provision on algorithmic decisions.[27] A data protection regime also exists for the EU institutions themselves (hereinafter: EU Data Protection Regulation[28]).

As for ETIAS, the legislators included specific provisions in the Regulation regarding the data protection rules applicable to safeguarding personal data:

- The EU Data Protection Regulation applies to the processing of personal data by the European Border and Coast Guard Agency and eu-LISA;
- The GDPR applies to the processing of personal data by the ETIAS National Units assessing applications, by border authorities and by immigration authorities;
- The Law Enforcement Directive applies to situations where the processing of personal data by the ETIAS National Units is performed by competent authorities assessing applications for the prevention, detection or investigation of terrorist offences or other serious criminal offences;
- The GDPR applies to situations where the ETIAS National Unit decides on the issue, refusal, revocation or annulment of a travel authorization;
- The Law Enforcement Directive applies to the processing of personal data by Member States' designated authorities for the purposes of consultation of data stored in the ETIAS Central System for the prevention, detection and investigation of terrorist offences or of other serious criminal offences by Member States' designated authorities and Europol;
- Finally, the processing of personal data by Europol pursuant to Articles 29 and 53 of the ETIAS Regulation falls under the rules of the Europol Regulation.[29]

It is understandable that these rules need to be applicable in a complementary way. Although the ETIAS undeniably relates to law enforcement, it can be argued that the Law Enforcement Directive does not *generally* apply to the ETIAS, as the ETIAS concerns *predictive* immigration measures based on risk indicators and is thus not (or not necessarily) connected to actual criminal offences. Similarly, the GDPR is not *generally* applicable to the ETIAS (which aims to improve public security via immigration control) as it is generally not applicable to the processing of personal data by authorities for the purposes of the prevention, investigation,

[26]GDPR, art 2 (d).

[27]Directive (EU) 2016/680 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 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 [2016] OJ L119/89.

[28]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 [2018] OJ L295/39.

[29]Chapter VI of the Europol Regulation contains specific, detailed data protection safeguards concerning the work of Europol. See Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53, (Europol Regulation) arts 28–46.

detection or prosecution of criminal offences, including the safeguarding against and prevention of threats to public security.[30] Third, data processing by EU institutions needs to be covered by the relevant general or, in the case of Europol, special rules.

At first glance, it seems that the EU legislators have made an effort to cover the data protection aspects of the operation of the ETIAS. What is, however, not addressed in the ETIAS Regulation is to what extent the *automated* nature of the processing of personal data complies with various data protection regimes – or fundamental rights. Before we delve into this question, it is necessary to examine a highly significant and relevant judgment of the CJEU.

3. AUTOMATED DATA PROCESSING AND THE CJEU: *LIGUE DES DROITS HUMAINS*

As is often the case in EU law, the precise scope of certain provisions or requirements only becomes entirely clear in the light of the interpretation by the Court of Justice of the EU (CJEU). Concerning data processing and the ETIAS, one cannot disregard the judgment of the CJEU in Case C-817/19 *Ligue des droits humains*, also known as the 'PNR judgment'.[31]

Passenger Name Records, or PNR, are processed in relation to air passengers on extra-EU flights entering and leaving the European Union in line with the EU PNR Directive for the purposes of combating terrorist offences and other serious crimes.[32] A Belgian human rights organization, *Ligue des droits humains,* brought an action before the Belgian Constitutional Court in order to have the Belgian law transposing the PNR directive annulled.[33] The organization claimed – *inter alia* – that the law violated the Charter, specifically Articles 7 (respect for private and family life), 8 (protection of personal data) and 52(1) (limitation of rights).

The PNR Directive requires the collection of various pieces of data, including travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation number, passenger contact information, information relating to the means of payment or billing, information concerning baggage and general remarks regarding passengers, with the data collected pertaining to identified individuals – thus the processing of this data may indeed affect the right to respect for private life as per Article 7 CFR.[34] It was found by the CJEU that the right

[30]GDPR, art 2 (d).

[31]Case C-817/19 *Ligue des droits humains v Conseil des ministres* (ECJ, 21 June 2022). The judgment will not be analysed in full, but only as to its specifically relevant elements. It should also be noted briefly that the CJEU had previously had the opportunity to examine Passenger Name Record-related legal rules, specifically in the context of the EU-Canada PNR agreement. In its Opinion 1/15 [EU: C:2017:592], the CJEU ruled that the agreement on the transfer and processing of PNR data was incompatible with the Charter (specifically Articles 7, 8, 21 and 52(1)) insofar as it does not preclude the transfer and retention of sensitive data from the EU to Canada.

[32]Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119/132.

[33]Case C-817/19, para 51.

[34]Case C-817/19, paras 93–94.

to personal data protection was also affected, as the processes prescribed by the PNR Directive entailed the retention and transfer of such data.[35] In summary, the CJEU held that the PNR Directive, as it set out 'to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services', represented interference with Article 7 and 8 rights.[36] However, the Court upheld the validity of the PNR Directive precisely because the Charter guaranteed that the Directive respected relevant fundamental rights, if interpreted and applied correctly.[37] That being said, the CJEU did lay down a number of safeguards applicable to data processing within the framework of the PNR directive – and, as will be argued below, possibly elsewhere.

Among these safeguards, the CJEU conducted an evaluation of the advance assessment of PNR data by automated processing. According to the PNR Directive, the so-called advance assessment is carried out in two steps: first, the relevant national authority (passenger information unit, PIU) processes PNR data by automated means by comparing it against information held in databases or pre-determined criteria; second, in cases where the automated processing leads to a 'hit', the PIU shall, pursuant to Article 6(5) of the PNR Directive, carry out an individual review by non-automated means to verify whether further action by competent authorities is necessary.[38] Herein, the CJEU foresaw a 'fairly substantial' margin of error since the processing was carried out on the basis of unverified personal data: the CJEU underlined that no decision that produces an adverse legal effect on a person or significantly affects a person may be taken by the competent authorities only by reason of the automated processing of data.[39] More specifically, as regards comparing PNR data against information held in databases, the CJEU stressed that any such database needed to be non-discriminatory, i.e., based on objective and non-discriminatory factors;[40] it further held that relevant PNR data may only be checked against databases regarding persons or objects sought or under alert and not any other ones (e.g. those managed by private persons), and must be limited to what is strictly necessary for the purposes of combating terrorist offences and serious crime. The latter should ensure the targeted, proportionate and specific nature of the pre-determined criteria against which the data will be checked.[41] The CJEU further stressed that as the PNR Directive includes the checking of data against *pre-determined* criteria, this precludes the use of machine learning systems (which, by the way, are AI-based): i.e., systems which are self-learning and capable of modifying the monitored criteria or other elements of the assessment process without human intervention.[42] The 'opacity' of artificial intelligence-based systems would also render the individual review of positive 'hits' redundant, as it would not be possible to determine the exact reasons for a positive

[35]Case C-817/19, paras 95–96.

[36]Case C-817/19, para 111.

[37]Case C-817/19, para 228.

[38]Case C-817/19, para 176–177.

[39]Case C-817/19, para 178–179.

[40]Case C-817/19, para 189–190.

[41]Case C-817/19, para 190–191.

[42]Case C-817/19, para 194.

match from an adaptive automated system; this would also divest individuals of effective judicial remedy.[43]

The CJEU's judgment in *Ligue des droits humains* represents an important milestone regarding (among other things[44]) the judicial review of automated decision-making and data processing. The CJEU's postulates, as mentioned above, can be interpreted as a *de facto* ban on machine learning systems in the EU security architecture pertaining to data processing.[45] The reasoning of the Court – i.e. that no decision that produces an adverse legal effect on a person or significantly affects a person may be taken by the competent authorities only by reason of the automated processing of data – mirrors the requirement enshrined in the GDPR vis-à-vis automated decision-making (Article 22) and in the sister provision of the EU Data Protection Regulation (Article 24); thus even where these secondary rules may not apply as such, the Court saw the necessity to adopt the aforementioned requirement as binding.

As regards interference with fundamental rights, the CJEU applied the 'strictly necessary' test, building upon its earlier Opinion 1/15, requiring the strict proportionality of the interference.[46] As to the preclusion of self-learning or machine learning systems, the main argument that the CJEU relied upon was that such systems can modify the assessment process without human intervention, rendering the procedure opaque to data subjects concerning the actual reasons for the decision, thereby making effective judicial remedy questionable.[47]

4. IN LIGHT OF THE FOREGOING: AUTOMATED DATA PROCESSING IN THE ETIAS

Although seemingly different in their goals (the PNR system is meant to assist in combating terrorist offences and other serious crimes, while the ETIAS serves much broader purposes of promoting security, counter-migration and public health[48]), many similarities still exist. Similarly to the PNR Directive, ETIAS also aims to introduce a continuous, untargeted and systematic surveillance regime.[49] It is important to see that the ETIAS will work on the basis of risk indicators, where the specific risks have been further defined by the European Commission in a delegated act,[50] and will have to be 'specified' in a Commission implementing act – but the specific risk *indicators* themselves will be determined by FRONTEX as the central unit of the ETIAS. It will be these risk indicators that will enable the algorithmic profiling of individuals by

[43]Case C-817/19, para 195.

[44]For instance, the relevance of the judgment regarding data protection rules applicable to cooperation between the public and private entities in personal data sharing could also be mentioned. See Guild and Molnar (2023).

[45]Kuşkonmaz (2023) 311.

[46]Brouwer (2023a) 849–50.

[47]Brouwer (2023a) 855–57.

[48]Vavoula (2022) 468.

[49]Cf. Case C-817/19, para 111 and, regarding its applicability to ETIAS: Musco Eklund (2022).

[50]Commission, 'Delegated Decision of 23.11.2021 on further defining security, illegal immigration or high epidemic risks' COM (2021) 4981 final (Delegated Decision of 23.11.2021).

filtering and processing the personal data provided by users of ETIAS themselves. The ETIAS Regulation requires that risk indicators be targeted, proportionate, and non-discriminatory; however, this arguably still leaves rather broad discretion for FRONTEX regarding how to define them, as it is not specified how personal data or even traits need to be weighed against each other in the risk assessment.[51] It has been argued that leaving the risks and risk indicators to be used in the ETIAS undefined in the Regulation itself allows the EU executive and an EU agency (FRONTEX) to determine the results, with insufficient legal safeguards and possibly uneven interpretation.[52]

At this time, a thorough outline of the exact logic of algorithmic processing used in the ETIAS is not available, although it can be ascertained that the profiling will be based on sets of characteristics, which the delegated act defines as distinguishable sets of observable qualities or properties based on information and statistics.[53] Such a process could lead to issues: for instance, data on nationality and residence matched against data on age, sex, education and occupation could lead to discriminatory profiling as specific groups of third-country nationals may be at risk of being categorized based on the relative weight of their current occupation or level of education, and the correlation of said data with, for example, data on gender.[54] Unjustified profiling and indirect discrimination could also result from a combination of data on, for example, a specific ethnic group or nationality typically working in a given economic sector (such as construction) from a particular country, which may unjustly result in the refusal of travel authorization.[55] Incidents involving automated decision-making and supposedly neutral factors resulting in both direct and indirect discrimination have already been reported in the EU.[56]

There is furthermore no regulation on how the seriousness, or rather the relative weight of various risk indicators vis-à-vis each other shall be determined, nor do there seem to be measures for dealing with the possible overrepresentation of specific characteristics in certain groups of travellers (which could result in others possessing some of these characteristics unfairly being considered high risk).[57] Based on the PNR judgment analysed above, the CJEU requires that the data subjects shall be 'able to understand how those criteria and those programs work, so that it is possible for that person to decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress'.[58] However, as Kuşkonmaz points out, an algorithm interpretable by laymen is indeed rather difficult (though not impossible) to conceive of, especially bearing in mind that AI-based algorithms are designed to evolve

[51] Musco Eklund (2022).

[52] Primorac et al. (2023).

[53] Delegated Decision of 23.11.2021, art 2 (b).

[54] Gugliotta and Elbi (2023) 8.

[55] European Union Agency for Fundamental Rights (2018) 117.

[56] Brouwer (2023b). For an exploration of AI, machine learning and discrimination in general, see: Allen and Masters (2020).

[57] Gugliotta and Elbi (2023) 8–9.

[58] Case C-817/19, para 210.

and are being constantly 'fed' new data, further complicated by the reference by authorities to security reasons for justifying the non-disclosure of detailed information.[59] It is also noteworthy that, at this point, it is not possible to determine the relative weight of the outcome of automated processing and human review, thus raising the risk of automation bias.[60]

In response to queries by researchers who have requested detailed information on the workings of the algorithms within ETIAS, FRONTEX stated that ETIAS will not rely on machine learning or AI, but rather 'filtering queries', yet according to a deep analysis of the processes of the ETIAS based on available data contrasted against the functioning of relevant EU systems by Derave et al., it can instead be concluded that ETIAS will not only serve as the next building block in the surveillance architecture of the EU, but unfortunately involves the risk of indirect discrimination vis-à-vis certain protected characteristics and, as mentioned, automation bias in the decision-making process, even with a human in the loop.[61] Further, the opacity of AI systems, as mentioned above by the CJEU in *Ligue*, will not only make it difficult for individuals to understand the logic behind decisions: it may potentially also affect the 'human in the loop', i.e., the human carrying out the review who must make decisions based on the 'hits' in the ETIAS, raising the question whether such review can be truly meaningful and actionable.[62] Regulating human decision-making in the process and preventing its 'displacement' by (faulty) algorithms should fall to the legislature, which possesses the necessary democratic legitimacy, not merely executive power.[63] Having regard to all of the above, it is uncertain whether the algorithmic aspect of the ETIAS actually complies with the *Ligue des droits humains* requirements, or in fact, those specified earlier in the PNR Opinion mentioned above, or the *Quadrature due net* judgement.[64]

The ECJ has recently had the opportunity to rule specifically on the interpretation and extent of the EU law limits on automated decision-making and profiling.[65] In *SCHUFA Holding*, the Court of Justice clarified, in the context of credit scoring, the cumulative conditions under which Article 22 of the GDPR applies: there must be a 'decision', this decision must be based solely on automated processing and must either have legal effects concerning the data subject or affect him or her 'similarly significantly.'[66] It is also clear from the judgment that the Court considers profiling (Article 4(4) GDPR) to be a sub-category of automated decision-making under Article

[59]Kuşkonmaz (2023) 314–15.

[60]Gugliotta and Elbi (2023) 10.

[61]Derave et al. (2022) 418–19.

[62]Gugliotta and Elbi (2023) 13.

[63]Thönnes and Vavoula (2023).

[64]Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier Ministre and Others [2020] (ECJ, 6 October 2020)*, which also concerned automated data analysis and combating terrorism. Cf. Derave et al. (2022) 408.

[65]Case C-634/21 SCHUFA Holding (ECJ, 7 December 2023). For an account of and reflection on the oral hearing of the preliminary ruling, see: Häuselmann (2023).

[66]Case C-634/21, para 43.

22 GDPR, and that decisions taken by AI based on personal characteristics or behaviour fall within the definition of profiling as defined by the GDPR.[67]

The 'black box effect', i.e. the opacity of the algorithm used by ETIAS, raises further similar concerns about the right to effective judicial review as those identified with the PNR system – yet the CJEU has held in its review of that very system that the right to effective judicial remedy was paramount – the 'constitutional anchor' of such decision-making, if you will.[68]

5. CONCLUDING REMARKS

The European Union aims to act as a trendsetter in the regulation of AI: this is clearly demonstrated by its adoption of the first-ever binding law on AI systems in the form of the AI Regulation originally proposed by the European Commission in 2021 as part of the EU's digital strategy.[69] The AI Regulation, having regard to the varying severity of possible effects on individuals' security and fundamental rights, utilizes a risk-based approach:[70] i.e., what the draft regulation requires of AI systems depends on the risks involved in the use of the AI system in question.[71] According to the regulation, high-risk AI systems must comply with specific requirements, including establishing a risk management system and ensuring human oversight and transparency.[72] Quite rightly so, the regulation categorizes the use of AI in the context of border control, migration and asylum as high-risk,[73] since the conduct and decisions of the authorities often concern people in particularly vulnerable positions and who are dependent on the outcome of the actions of the authorities.[74]

Yet, in a way, the EU seemed to be contradicting its own (future) AI standards by proposing to expressly excluding the ETIAS from the scope of the proposed AI regulation, along with other large-scale IT databases used in its justice and home affairs policy, also known as the Area of Freedom, Security and Justice.[75] This would have excluded the 'trustworthy AI' concept

[67] Winklbauer (2024).

[68] Kuşkonmaz (2023) 319.

[69] European Commission (2020).

[70] Mezei and Träger (2022) 23.

[71] See especially Chapter III and Annex III of the AI Regulation.

[72] AI Regulation, arts 8–15.

[73] AI Regulation, art 6(2) and Annex III. As has been noted, AI systems used in the implementation of the management of these policies affect individuals who are often in a particularly vulnerable situation and whose status is fundamentally affected by the outcome of the decision taken in the context of border control, migration management or asylum law. See (regarding the draft AI Regualtion) Mezei and Bán-Forgács (2022) 77.

[74] The preamble of the original proposal of the AI Regulation submitted by the Commission [COM(2021) 206 final] underlined this explicitly in para (39) in the context of migration, asylum and border control, stating that '[th]e accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration.' The preamble of the adopted Regulation no longer includes these aspects, but rather refers to such aspects in the context of the 'misuse' of AI systems [AI Regulation, preamble para (28)].

[75] Proposal for harmonised rules on artificial intelligence, COM(2021) 206 final, art 83 and Annex IX.

championed by the EU from very significant (actual or possible) fields of application.[76] In the end, the adopted AI Regulation chose a different path: instead of exclusion, it gave AI systems which are components of large-scale IT systems operating in the AFSJ that have been placed on the market or put into service before 2 August 2027 a significant compliance delay – such systems will only have to comply with the rules of the AI Regulation until 31 December 2030.[77] The ETIAS will no doubt also fall within this category. It is commendable that in the end, the EU chose not to favour its owns systems too much, although the compliance delay is also significant, especially when taking into account that other AI systems need to comply with the AI Regulation in timeframes ranging from six months to two years from entry into force of the regulation.[78]

It is also quite telling that attempts by various researchers to obtain detailed information on the exact functioning of the ETIAS screening algorithm directly from the relevant agencies have ultimately failed, highlighting a lack of transparency.[79]

It is commendable that ETIAS has a Fundamental Rights Guidance Board that includes the participation of, among others, the EU Fundamental Rights Agency, which performs regular appraisals and issues recommendations regarding the functioning of the ETIAS,[80] although a commitment for this body to regularly evaluate and – if necessary – propose modifications to the algorithm could have been made explicit in the Regulation.[81] What is more, in an age where a 'creep' toward algorithmic decision-making in public administration[82] and automated adjudication has been observed and criticized[83] in a context much broader than migration security (and possibly at odds with the right to a fair trial), it would be preferable for fundamental rights considerations regarding algorithmic decisions and the definition of specific risk indicators to be taken into account before the system becomes operational. This could be achieved by drafting legal safeguards that are at least theoretically capable of ensuring full compliance with the Charter. Based on the current state of play, as analysed above, that does not seem to be the case.

ACKNOWLEDGEMENT

The research was conducted within the framework of the Hungarian Ministry of Justice's programmes to improve the quality of legal education.

[76] Derave et al. (2022) 419.

[77] AI Regulation, art 111 and Annex X.

[78] Derave et al. (2022) 419.

[79] Cf. Derave et al. (2022) and Musco Eklund (2022).

[80] ETIAS Regulation, art 10 (1).

[81] Vavoula (2021) 472.

[82] Kollár (2022) 24.

[83] Pasquale (2021).

LITERATURE

Allen, R. and Masters, D., 'Artificial Intelligence: the right to protection from discrimination caused by algorithms, machine learning and automated decision-making' (2020) 20 ERA Forum 585–98.

Brouwer, E., 'Ligue des droits humains and the validity of the PNR Directive: Balancing individual rights and State powers in times of new technologies' (2023a) 60 Common Market Law Review 839–62.

Brouwer, E., 'Challenging Bias and Discrimination in Automated Border Decisions: Ligue des droits humains and the Right to Effective Judicial Protection', *Verfassungsblog* (11 May 2023b) <https://verfassungsblog.de/pnr-border/> accessed 21 October 2023.

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

Dombrava, C., 'Artificial intelligence at EU borders. Overview of applications and key issues, *European Parliamentary Research Service* (July 2021) <https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf> accessed 20 October 2023.

Duić, D. and Rošić, M., 'Interoperability between the EU information systems – from an idea to the realisation' (2022) 31 Policija i sigurnost 118–48.

European Commission, *Shaping Europe's Digital Future* (Publications Office of the European Union 2020) <https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf> accessed 21 October 2023.

European Union Agency for Fundamental Rights, *Preventing unlawful profiling today and in the future: a guide* (Publications Office of the European Union 2018) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf> accessed 20 October 2023.

Gerards, J., 'The fundamental rights challenges of algorithms' (2019) 37 Netherlands Quarterly of Human Rights 205–209.

Gugliotta, L. and Elbi, A., 'Will AI "subtly" take over decision-making in the EU migration context? Warnings and lessons from ETIAS and VIS' (2023) Jean Monnet Network on EU Law Enforcement Working Paper Series <https://jmn-eulen.nl/wp-content/uploads/sites/575/2023/06/7.-WP-Gugliotta-Elbi.pdf> accessed 21 October 2023.

Guild, E. and Molnar, T., 'The European Legal Architecture on Security: New Developments in the Complex Relationship Between the Public and Private Sectors in Data Processing', *Verfassungsblog* (10 May 2023) <https://verfassungsblog.de/pnr-architecture/> accessed 21 October 2023.

Häuselmann, A., 'The ECJ's First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber', *European Law Blog* (20 February 2023) <https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/> accessed 21 October 2023.

Kis Kelemen, B. and Hohmann, B., 'Is there new under the sun? A glance at the Digital Services Act and the Digital Markets Act from the perspective of digitalization in the EU' (2023) 19 Croatian Yearbook of European Law and Policy 225–48.

Kollár, G., 'A mesterséges intelligencia alkalmazásának adatvédelmi aggályai a közigazgatásban' (Data protection concerns regarding the use of artificial intelligence in public administration) (2022) 3 Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok 5–27.

Kuşkonmaz, E. M., 'The Grand Gala of PNR Litigations: Case C-817/19, Ligue des droits humains v Conseil des Ministres' (2023) 19 European Constitutional Law Review 294–319.

Mezei, K. and Bán-Forgács, N., 'Discrimination in the age of algorithms' in Florek, I., Laki, I. and Schottner, K. (eds), *Human rights as a guarantee of smart, sustainable and inclusive growth* (Milton Friedman University and Alcide De Gasperi University of Euroregional Economy 2022) 73–80.

Mezei, K. and Träger, A., 'The European Approach to Artificial Intelligence: Ethical and Regulatory Implications' (2022) 11 Acta Universitatis Sapientiae Legal Studies 19–34.

Musco Eklund, A., 'Frontex and 'Algorithmic Discretion' (Part I): The ETIAS Screening Rules and the Principle of Legality', *Verfassungsblog* (10 September 2022) <https://verfassungsblog.de/frontex-and-algorithmic-discretion-part-i/> accessed on 21 October 2023.

Pasquale, F., 'Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication' in Micklitz, HW., Pollicino, O., Reichman, A., Simoncini, A., Sartor, G. and De Gregorio, G. (eds), *Constitutional Challenges in the Algorithmic Society* (CUP 2021) 42–56.

Primorac, Ž., Bulum, B. and Pijaca, M., 'New European Approach on Passengers' Digital Surveillance through Electronic Platform (Etias) – Passengers' and Carriers' Perspective' (2023) 7 EU and Comparative Law Issues and Challenges Series 273–94.

Reichel, D. and Molnár, T., 'Big data, big responsibility – fundamental-rights implications of using artificial intelligence in migration management: A European perspective' in Rango, M., Sievers, N. and Laczko, F. (eds.), *Harnessing Data Innovation for Migration Policy: A Handbook for Practitioners* (International Organization for Migration 2023) 158–70.

Ritó, E., 'Mesterséges intelligencia az Európai Unió stratégiai és szabályozási dokumentumainak tükrében' (Artificial intelligence in the context of the European Union's strategic and regulatory documents) (2021) 2 Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok 33–47.

Thönnes, C. and Vavoula, N., 'Automated predictive threat detection after Ligue des Droits Humains: Implications for ETIAS and CSAM (Part II)', *Verfassungsblog* (12 May 2023) <https://verfassungsblog.de/pnr-threat-detection-ii/> accessed 21 October 2023.

Vavoula, N., 'Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' (2021) 23 European Journal of Migration and Law 457–84.

Vavoula, N., *Immigration and Privacy in the Law of the European Union* (Brill 2022).

Winklbauer, S., 'CJEU ruling in the matter of "SCHUFA" not only affects credit scoring (C-634/21)', *EuroCloud News* (25 April 2024) <https://eurocloud.org/news/article/cjeu-ruling-in-the-matter-of-schufa-not-only-affects-credit-scoring-c-63421/> accessed 18 July 2025.

LINKS

Link1: 'What is the New Pact on Migration and Asylum of the EU?' (*European Commission*) <https://home-affairs.ec.europa.eu/policies/migration-and-asylum/new-pact-migration-and-asylum_en> accessed 20 October 2023.

Link2: 'The Bratislava Declaration', *European Council* (16 September 2016) <https://www.consilium.europa.eu/media/21250/160916-bratislava-declaration-and-roadmapen16.pdf> accessed 20 October 2023.

Link3: 'Revised timeline for the EES and ETIAS', *European Union* <https://travel-europe.europa.eu/bg/etias/about-etias/news-corner/revised-timeline-ees-and-etias> accessed 18 July 2025.

Other documents

'Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security' COM (2016) 205 final.

'Delegated Decision of 23.11.2021 on further defining security, illegal immigration or high epidemic risks' COM (2021) 4981 final.

'Proposal for a regulation of the European Parliament and the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM (2021) 206 final.

'Communication from the Commission on a New Pact on Migration and Asylum' COM (2020) 609 final.

Case C-634/21 *SCHUFA Holding and Others*.

Case C-817/19 *Ligue des droits humains v Conseil des ministres* (ECJ, 21 June 2022).

Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119/132.

Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier Ministre and Others [2020] (ECJ 6 October 2020)*.

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 [2016] OJ L119/1.

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 [2017] OJ L327/20.

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 [2018] OJ L236/1.

Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 [2018] OJ L295/99.

Regulation (EU) 2019/1896 of the European Parliament and of the Council on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 [2019] OJ L 295/1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L1689/1.