BRILL
NIJHOFF

EUROPEAN JOURNAL OF MIGRATION
AND LAW 23 (2021) 485–507

European
Journal of
Migration
and Law

brill.com/emil

Schengen and the Administration of Exclusion: Legal Remedies Caught in between Entry Bans, Risk Assessment and Artificial Intelligence

Evelien Brouwer
Lecturer in Public Law and Technology, Institute of Jurisprudence, Constitutional Law and Administrative Law – Montaigne Centre for Rule of Law and Administration of Justice, Utrecht University, Utrecht, The Netherlands
e.r.brouwer@uu.nl

Abstract

To create an area in which persons can move freely, the Schengen states committed to control their external borders to prevent irregular immigration and the entry of third-country nationals (TCNs) who are considered to be 'a public order and security risk'. The exclusion of 'unwanted aliens' can be based on the mutual enforcement of national decisions, such as entry bans reported in the Schengen Information System, or objections against the issuing of a Schengen visa, based on the consultation procedure in the Visa Code. This contribution focuses on the right of TCNs to have access to effective remedies, both with regard to existing and newer mechanisms of exclusion. It argues that when dealing with the use of large-scale databases and risk assessment as basis for excluding admission, existing rules and case-law by the CJEU should be taken into account to ensure access to effective judicial protection for TCNs.

Keywords

SIS II – Visa Code – risk assessment – mutual trust – Artificial Intelligence – algorithms – effective remedy – entry bans – ECRIS-TCN – ETIAS

1 Introduction

To create an area in which persons can move freely, the Schengen states engaged to control their external borders, preventing irregular immigration and the entry of persons who are considered to be a public order and security risk. For this purpose, the EU legislator developed different mechanisms to exclude those considered as either a security or irregular immigration risk. These measures can be based on first, the mutual enforcement of national decisions from other Member States and second, a prior risk assessment of third-country nationals (TCNs). A well-known example of the first exclusionary tool, is the reporting of inadmissible TCNs in the Schengen Information System (henceforth SIS) on the basis of the SIS II Regulation.[1] Another example is the mutual recognition of national objections against the issuing of a short-term visa to TCNs, following the consultation procedure in accordance with the Visa Code.[2] A third, and more recent, example concerns the implementation of the new ECRIS-TCN Regulation.[3] This database, set up for judicial cooperation, will include information on TCNs with a criminal record in one of the EU Member States. As we will see below, the Regulation explicitly allows Member States to use information based on criminal convictions in other states, for the purpose of asylum and immigration control.

Addressing the second example of exclusion, it is clear that in the future, EU Member States will make much more use of prior risk assessment, including the use of artificial intelligence and algorithms. Decision-making with regard to short-term visa applications in accordance with the Visa Code, is already based on prior consultation of existing large-scale databases and data analysis, in order to define the trustworthiness or 'risk' of the applicant. On the basis of the new ETIAS Regulation, risk assessment will also be applied to

1 Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L381. For the consolidated version of the SIS II Regulation, see <http://data.europa.eu/eli/reg/2006/1987/2020-12-28> accessed 8 October 2021.

2 Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) [2009] OJ L243. For the consolidated version of the Visa Code, see <https://eur-lex.europa.eu/eli/reg/2009/810/2020-02-02> accessed 8 October 2021.

3 Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 [2019] OJ L135.

visa-exempted TCNs who will have to apply for a travel authorisation before visiting the Schengen territory.[4] Furthermore, with the Migration Pact, presented in September 2020, the European Commission submitted a proposal for the pre-screening of third country nationals at the external borders of the EU, on the basis of which border guards can 'flag' a person who is considered as a security threat.[5] Plus, in the proposal to regulate the use of artificial intelligence, the Commission even explicitly envisages the use of polygraphs or lie-detectors within the field of not only criminal law, but also asylum and migration law decision-making.[6]

From the perspective of the right to have access to legal remedies, these developments raise several issues for concern. Currently, TCNs already encounter practical and legal problems when being refused entry or a visa on the basis of a SIS alert, when such an alert has been issued by another state than the state denying entry or a short-term visa. These same problems may arise for visa applicants whose short-term visa has been refused based on an objection from another Member State. These problems are related to a lack of transparency concerning not only the reasons for refusal, but also which State is responsible for the 'entry ban' and where to lodge an appeal. In light of the new mechanisms of exclusion proposed by the Commission, which are based on risk assessment including the use of algorithms, it is much more difficult for TCNs to know and address the reasons for refusal in an effective way. In this contribution, I will describe the right of TCNs to have access to effective remedies, both with regard to existing and newer mechanisms of exclusion. I will argue, that when dealing with the use of large-scale databases and risk assessment as basis for excluding admission, existing rules and case-law by the CJEU should be taken into account to ensure access to effective judicial protection for TCNs.

The first part of this contribution, describes existing and future instruments of mutual exclusion as provided in the Schengen Information System (SIS), the exclusion of TCNs based on the consultation mechanism in the Visa Code,

4 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.

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum, COM/2020/609 final.

6 Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final, Brussels, 21.4.2021.

and the use of ECRIS-TCN for immigration purposes. Secondly, I will give an overview of new mechanisms allowing further use of risk assessment and profiling, including for example the pre-screening proposal and the flagging of security risks. Finally, I will briefly address the proposed use of polygraphs in the Artificial Intelligence proposal. In the third part, I will discuss the right to effective remedies, first by describing the specific laws as dealt with in this contribution and second, based on case-law by the CJEU. In the conclusion, I will identify the relevant minimum standards for the right to effective remedies for TCNs reported, flagged, or simply considered as unwanted by the Schengen states.[7]

2 No Admission: The Mutual Recognition of National Decisions

2.1 *SIS II Alerts for the Purpose of Refusal of Entry*

On the basis of the Schengen Borders Code and Visa Code, entry, respectively the issuing of a short-term visa, must be refused to a person who is registered into SIS II by one of the Member States for the purpose of refusal of entry.[8] This use of SIS is thus based on mutual recognition of, and trust in, national decisions of the other state submitting the SIS alert. In accordance with the current SIS II Regulation, a person may be reported as inadmissible in SIS II, first, if he or she is considered as a threat to public policy or public security or national security, for example if the person is convicted by a Schengen state for a crime punishable with a deprivation of liberty for at least one year. Second, a SIS alert may be based on the fact that the person is the object of a restrictive measure intended to prevent entry into or transit through the territory of Member States, including those implementing a travel ban issued by the Security Council of the United Nations. Third, a SIS alert for the refusal of entry will be entered into SIS II if the TCN has been subject to a decision of expulsion, refusal of entry, or removal.

7 I use the term 'unwanted' even if this is not a legal term, to emphasize the discretionary power to declare third-country nationals as inadmissible on the basis of the current Schengen rules, see also Elspeth Guild referring to 'unwanted foreigners' in her farewell speech. Elspeth Guild, 'Interrogating Europe's Borders: Reflections from an Academic Career' (Radboud Universiteit Nijmegen 2019) 12.

8 Article 6 (1) (d) Regulation 2016/399 (Schengen Borders Code) and Article 32 (a) (v) Regulation 2019/1155 amending Regulation 810 (200) (Visa Code).

Both the goal and the content of SIS II have been extended by several Regulations adopted in June 2018. Regulation 2018/1861[9] on the use of SIS for border controls, allows further storage of biometrics and a new category of alerts on third country-nationals in SIS II, namely persons 'circumventing national law on entry or stay'. Furthermore, Regulation 2018/1860[10] provides for the obligatory storage of return decisions issued on the basis of the Return Directive 2008/115.[11] These amendments will become binding on the basis of an implementing decision of the Commission which must be adopted no later than 21 December 2021.[12]

Regulation 2018/1861 maintained two important restrictions with regard to the issuing of a SIS alert for the purpose of refusal. First, Article 21, obliges Member States to, before entering a SIS alert, assess its proportionality and to determine whether the case is 'adequate, relevant and important enough' to warrant an alert in SIS. This proportionality test requirement however, does not apply to SIS alerts related to a terrorist offence (on the basis of Article 24 (2) (b)), as they are, according to Article 21 (2), in itself considered as 'adequate, relevant and important enough'. Second, SIS alerts must be based on an individual assessment. This assessment implies in accordance with Article 24 (1), that states are required to make an individual assessment of the personal circumstances of the individual and the consequences of refusing him or her entry to the territory. The individual assessment requirement does not apply for the issuing of entry bans on the basis of Return Directive, but, here one could argue that legally even a stricter requirement applies to entry bans following the Return Directive. In the judgment *Zh. and O*, the CJEU has held that states, deciding within the framework of Article 7(4) of the Return Directive whether or not to grant the person a period of voluntary return or to issue an entry ban, must decide on a case-by-case basis, in order to ascertain whether

9 Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 [2018] OJ L312.

10 Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals [2018] OJ L312.

11 Before this amendment adopted in 2018, the reporting of entry bans following a return decision had no explicit legal basis, but was mentioned in recital 18 of the Return Directive, see Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals [2008] OJ L348.

12 See respectively Articles 79 Regulation 2018/1862 and Articles 20 Regulation 2018/1860 and 66 (2) Regulation 2018/1861.

the personal conduct of the TCN concerned poses a genuine and present risk to public policy.[13] According to the CJEU, when a Member State relies 'on general practice or any assumption in order to determine such a risk, without properly taking into account the national's personal conduct and the risk that that conduct poses to public policy', it fails to have regard to the requirements relating to an individual examination of the case concerned and to the principle of proportionality. Generally, however, due to the lack of harmonized criteria, Member States retained a wide discretionary power to report TCNs for the purpose of refusal of entry in SIS.[14]

Currently, the Member States also use the SIS to issue alerts on so-called Foreign Terrorist Fighters (FTF) based on information from third states. These alerts are either based on Article 24 (2) (b) Regulation 2018/1861, on persons related to terrorist offences, for the purpose of refusal of entry, or on Article 36 Regulation 2018/1862 for the purpose of 'discreet, inquiry of specific checks'.[15] Such information from 'trusted third countries', has already been entered into SIS by some 'willing Member States' (including the Czech Republic and Italy) according to a Presidency note of May 2020.[16] This means that when using SIS, the Member States do not only rely on each other's information on inadmissible TCNs or persons convicted or suspected for terrorist crimes, but also trust and use information from third states. In December 2020, the European Commission proposed to allow Europol to enter so-called 'information alerts' on TCNs into SIS.[17] Such alerts would be based on Europol's assessment concerning TCNs who are not protected by EU's freedom of movement, and whose behaviour falls within the scope of the crimes for which Europol has

13 Case C-554/13 *Zh. and O*, EU:C:2015:377, para 50.

14 That SIS alerts for the purpose of refusal of entry may even be related to political grounds, has been illustrated by the case of Mrs. Kozlovska, see Evelien Brouwer, 'Schengen Entry Bans for Political Reasons? The Case of Lyudmyla Kozlovska' (*Verfassungsblog*, 30 August 2018) <https://verfassungsblog.de/author/evelien-brouwer/> accessed 8 October 2021.

15 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU [2018] OJ L312.

16 Council doc. 6322/20, LIMITE, 26 February 2020. See also 'Balkan spies "feed" EU's database via Czech' (EU Observer 12 February 2020) <https://euobserver.com/justice/147420> accessed 8 October 2021.

17 COM (2020) 791, 9 December 2020. The Commission called this possibility an 'important paradigm change for SIS'.

the mandate to support the Member States.[18] This proposal did not receive sufficient support, as Member States found it unclear which action had to be taken on the basis of these Europol alerts. As compromise, in May 2021, the EU Presidency proposed to give Europol a supporting role with regard to the analysis and verification of third country information to be entered by Member States in SIS.[19] In view of the aforementioned conditions in the Schengen Borders Code and criteria as defined by the CJEU in the *Zh. and O.* case, this increasing involvement of Europol in migration decisions is problematic. This involvement will increase the lack of transparency in the decision-making process, making it more difficult to verify and scrutinize the sources and the legitimacy of the information being used. This problem of scrutiny is aggravated because as we have seen above, the required prior proportionality test does not apply to SIS alerts related to terrorist offences. Here again, the lack of a common interpretation of 'terrorist offences' and 'related to' may result in differentiated practices within the EU.

2.2 *The Consultation Mechanism in the Visa Code: Other States' Objections*

The Visa Code provides for a consultation procedure on the basis of which one Member State refuses a visa by reason of an objection issued by another Member State. In accordance with Article 22 Visa Code, a Member State may submit to the Commission a list of third countries, on the basis of which, whenever a person with the nationality of one of the listed states applies for a visa in another Member State, the latter state must consult the former state. If the consulted Member State subsequently objects against the issuing of a visa to this person, the visa will be refused even if he or she does not intend at all to visit the objecting state. This cooperation is implicitly based on mutual or interstate trust. Due to the use of the standard form set out in Annex VI of the Visa Code, the visa refusal does not provide much information on the reasons of refusal and the applicant may not even be informed about which state objected against the issuing of a visa.[20] In practice this means that when a

18 These crimes concern amongst others terrorism, organized crime, drug trafficking and money laundering, but also computer crime, corruption and immigrant smuggling, see Annex 1 to the Europol Regulation 2016/794 [2016] OJ L135.

19 Council document 9158/21, 28 May 2021, 5.

20 Annex VI, Point 6 Visa Code provides that a visa can be refused when one or more Member State(s) considers the applicant to be a threat to public policy, internal security, public health as defined in Article 2(19) of the Schengen Borders Code or the international relations of one or more of the Member States.

visa is refused following an objection of another Member State, the consulting state, nor the applicant may know the reasons for this objection.

According to Article 53 Visa Code, Member States should inform the European Commission of the third countries for which they require prior consultation in the context of a visa application. The European Commission issues a list containing these countries of origin.[21] By 2013 the list consisted of 30 third countries.[22] In the 2017 version, the list had expanded to 38 third countries.[23] The applicants subject to prior consultation are mostly nationals of African, Asian and Arabic-speaking states, including states 'producing' the highest number of refugees.[24] Stateless persons and refugees, regardless which nationality they hold, are included in the list as well.

2.3 *ECRIS-TCN and Its Use in Immigration and Asylum Decision-Making*

The ECRIS-TCN Regulation 2019/816, adopted in April 2019, provides for a centralized system containing information on TCNs following national decisions related to criminal convictions or prosecutions.[25] This may include criminal convictions of TCNs based on violations of national immigration laws. Following Article 7 of the Regulation, information in ECRIS-TCN can be requested for criminal proceedings or 'for any of the other purposes mentioned in this provision, if provided by national law'. These 'other purposes' may include security clearances, vetting for voluntary activities involving contacts with children or vulnerable persons, and also 'visa, acquisition of citizenship and migration procedures, including asylum procedures'. This means that national immigration and asylum authorities may, if provided by national law, check ECRIS-TCN and decide to use information on criminal records from other Member States in their immigration law decision-making.

In 2019, the Commission submitted a proposal explicitly allowing border guards to use the data included in ECRIS-TCN for the purpose of border

21 See the Migration Law Clinic expert opinion Access to legal remedies against a visa refusal based on an objection of another Member State prepared by students from the Vrije Universiteit Amsterdam for the Joined Cases C-225/19 and C-226/19 *R.N.N.S. and K.A.* (dealt with further below).

22 This list is published at the website of the Dutch Ministry of Foreign Affairs.

23 The list used to be published by the Commission, but now seems to have disappeared. See <https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/visa-policy/decision-visa-application_en> accessed 8 October 2021.

24 See UNHCR, 'Figures at a glance' <https://www.unhcr.org/figures-at-a-glance.html> accessed 8 October 2021.

25 See supra note 3.

management in accordance with the ETIAS Regulation 2018/1240.[26] As discussed below, once ETIAS becomes operational, persons from visa exempted countries will need a prior travel authorisation before arriving in the EU territory. The ECRIS-TCN proposal provides the use of information in ECRIS-TCN in border and immigration law decisions in general, but also to decide upon applications for travel authorisations by visa exempted TCNs. Different from the general provision in the ECRIS-TCN Regulation, access within the framework of the ETIAS Regulation would be limited to national records in ECRIS-TCN on TCNs convicted for a terrorist offence or another serious criminal offence. For this purpose, a proposed amendment of ECRIS-TCN Regulation provides in Article 5 for the addition of a 'flag' to the ECRIS-TCN that the TCN has been convicted either in the past 25 years for a terrorist offence or in the past 15 years for a serious criminal offence as listed in the Annex to Regulation 2018/1240. These latter offences should be punishable under national law by a custodial sentence or detention order for a maximum period of at least three years. The Commission thus proposes a higher threshold for applicants from visa exempt countries than for TCNs who need a short-term visa to enter the Schengen territory. Nevertheless, the lengthy periods during which convictions in the past will still result in the refusal of travel authorisation is worrying. Furthermore, the data retention period for information in ECRIS-TCN, including the aforementioned flags is entirely left to the national laws.[27]

In its opinion of 2015, the Fundamental Rights Agency (FRA) proposed an explicit prohibition of using ECRIS-TCN information for immigration law enforcement purposes outside criminal law proceedings.[28] The FRA warned against secondary effects from national convictions based on previous irregular entry or stay, which, specifically for refugees and children, would have adversary effects for their integration and protection. It further proposed to clearly define the system's purpose in a manner that limits the Member State's discretion. The added value of ECRIS-TCN with regard to the already existing option to report convicted or suspected TCNs into SIS is unclear and has not been substantiated by the EU legislator. As submitted by Vavoula, there will

26 COM (2019) 3, 7 January 2019, proposal for a Regulation establishing the conditions for access to the other EU information systems and amending Regulation 2018/1862 and the ECRIS-TCN Regulation. See also the amended proposal in Council document 7520/21, 31 March 2021.

27 See Article 8 of the current ECRIS-TCN Regulation: 'Each data record shall be stored in the central system for as long as the data related to the convictions of the person concerned are stored in the criminal records.' and Article 8 (2) of the proposed amendment.

28 FRA, 'Opinion 1/2015' <http://fra.europa.eu/en/opinion/2015/fra-opinion-exchange-information-third-country-nationals-under-possible-system> accessed 8 October 2021.

be complete overlap between SIS and ECRIS-TCN with regards to convictions on terrorist offences. Furthermore, the overlap between SIS and ECRIS-TCN with regards to other offences listed in the Annex of the ETIAS Regulation will be opaque due to the discretion enjoyed by Member States in registering such alerts.[29]

3 New Tools of Exclusion: Risk Assessments and Algorithms

3.1 *ETIAS and the Refusal of Travel Authorisation*

On 25 April 2018, the Council and the European Parliament reached an agreement on the European Travel and Authorisation System (ETIAS), proposed by the European Commission in 2016 for 'strengthening integrated border management and enhancing internal security'.[30] The ETIAS system, when operational, requires visa-exempt TCNs to apply for a travel authorisation and to submit personal information into an online application before travelling to the EU. Their data will be cross-checked against a number of databases and on the basis of this comparison a travel authorisation can be either issued or refused.[31] In addition to the aforementioned existing large-scale databases, the ETIAS Regulation provides for an additional information system, the ETIAS Central System (Article 6).

According to Article 37 of the ETIAS Regulation, a travel authorisation will be refused amongst others if the applicant poses a security, an illegal immigration, or a high epidemic risk, or he or she is a person in respect of whom an alert has been entered into SIS for the purpose of refusing entry or stay. Other refusal grounds include the fact that the applicant used a travel document which has been reported as lost, stolen misappropriated or invalidated in SIS, or for failing to reply to request to provide failing or additional documentation within ten days of the date of receipt of the request (Article 27 (2)). Aside from the aforementioned risk assessment, Article 37 allows national authorities to refuse a travel authorisation, if 'there are reasonable and serious doubts

29 Niovi Vavoula, 'The European Commission package of ETIAS consequential amendments. Substitute impact assessment', EPRS (Brussels 2019), 48 and 54, <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/642808/EPRS_STU(2019)642808_EN.pdf> accessed 8 October 2021.

30 Regulation 2018/1240 establishing a European Travel Information and Authorisation System [2018] OJ L236.

31 ETIAS is comparable to ESTA as established in the United States of America (USA) following the 9/11 terrorist events which concerns an online authorisation that EU and other visa-exempt citizens need to fill in prior to traveling to the USA.

as to the authenticity of the data, the reliability of the statements made by the applicant, the supporting documents provided by the applicant or the veracity of their contents'. This entails, in addition to the aforementioned refusal mechanisms on the basis of the SIS II Regulation, the Visa Code and the use of the ECRIS-TCN regulation, another quite discretionary and unspecified ground to deny TCNs admission to the EU.

To assess whether a person is eligible to enter the EU, three levels of information sorting will be used. First, an automated comparison will take place with national and EU databases, for example to check if travel documents have been reported as stolen, lost or invalidated in SIS or national databases, or if the person has been reported for the purpose of refusal of entry into the SIS. Second, there will be an assessment based on 'ETIAS screening rules'. According to Article 33, these rules are based on an algorithm enabling profiling through the comparison between the data recorded in an application file of the ETIAS Central System with specific risk indicators established by the ETIAS Central Unit pointing to irregular migration, security or public health risks. Third, the personal information of the applicant of the travel authorisation will be compared to the so-called ETIAS watchlist (Article 22). This list will be established on the basis of information provided by Europol 'related to terrorist offences or other serious criminal offences' (Article 34). Furthermore, Article 11 of the ETIAS Regulation provides for interoperability between the ETIAS Central System with other EU large-scale databases, including SIS II, Eurodac,[32] the Visa Information System or VIS,[33] ECRIS-TCN, and the Entry Exit System or EES,[34] for the purpose of the 'risk-assessment' of the application. Applications for a travel authorisation will be automatically processed, after which the ETIAS Central System examines 'each application file individually' (Article 20). The decision on the travel authorisation is taken by the 'ETIAS Central Unit' or the National Unit of the responsible Member State (Article 36). Once issued, the travel authorisation remains valid for five years.

32 Eurodac includes information on asylum seekers and third-country nationals who have crossed EU's borders on an irregular basis. It was originally set up for the implementation of the Dublin Regulation, but gradually the EU legislator extended its content and purposes meaningfully. See Eurodac Regulation 603/2013 [2013] OJ L180.

33 The VIS includes information on every decision adopted with regard to a short-term visa application by a third-country national on the basis of the Visa Code. See VIS Regulation 767/2008[2008] OJ L 218 as amended in 2021 by the Regulations 2021/1133 and 2021/1134 [2021] OJ L248.

34 The EES, when operational, will register the entry and exit of TCNs crossing the external borders of the EU. See, Regulation 2017/2226 [2017] OJ L327.

3.2 *Pre-screening and Security Flags in Eurodac*

Addressing new mechanisms of exclusion, it is important to refer in this contribution to the new 'pre-entry phase' as proposed in the Migration Pact of September 2020, ensuring the screening of TCNs (TCNs) arriving at EU's external borders.[35] The aim of the pre-entry phase is, according to the Commission, to establish a 'seamless link' between all stages of the migration process from arrival to processing of asylum requests and granting of international protection or, where applicable, the return of those not in need of protection.

On completion of the screening procedure, the responsible authorities should fill out a so-called 'de-briefing form', containing personal and very detailed information.[36] This information includes: name, date and place of birth and sex, initial indication of nationalities, countries of residence prior to arrival, languages spoken, reason for unauthorised arrival, entry, or illegal stay; information on whether the person made an application for international protection, information obtained on routes travelled and any other information on assistance received from a person or organisation in crossing the border without authorisation. The proposed screening procedure may result in four possible outcomes: 1) refusal of entry; 2) return; 3) asylum or; 4) relocation. As submitted by the organisation European Council on Refugees and Exiles (ECRE), the relationship between refusal of entry based on this proposed regulation and the Schengen Borders Code is unclear.[37] The added value of the screening procedure in addition to the already applicable border controls and the scrutiny of individuals at the external borders based on the Schengen Borders Code is therefore questionable.

Furthermore, the proposal includes the possibility to assess during the pre-screening procedure whether the TCN poses a possible security risk. This assessment is also provided for in Article 57 (7) of the proposed Regulation on Asylum and Migration Management in the procedure before relocation.[38] Based on the outcome of such a security assessment, national authorities must submit information to the Central System of Eurodac that the person could

35 Proposal for a Regulation introducing a screening of third-country nationals at the external borders, COM (2020) 612 (Screening proposal).

36 Article 13, Screening proposal.

37 ECRE, 'Comments on the Commission Proposal for a Screening Regulation Com (2020) 612' (Brussels 2020) 31–32 <https://ecre.org/wp-content/uploads/2020/12/ECRE-Comments-COM2020-612-1-screening-December-2020.pdf> accessed 8 October 2021.

38 COM (2020) 610.

pose a threat to internal security.[39] In order to delink this proposal from the negotiations on the other Migration Pact proposals, an amended version of the Eurodac Regulation of September 2021 no longer refers to the Screening Regulation.[40] The new proposal now provides that Member States must submit to Eurodac 'the fact that the person could pose a threat to internal security following security checks.' The content and the conditions under which such security checks may take place, is thus entirely left to the national rules and practices of the Member States. As this information will be retained for ten years in Eurodac, the outcome of these security checks may have long-term implications for TCNs, while possibly affecting the right to apply for international protection.[41]

3.3 *Regulating the Use of Artificial Intelligence and…. Polygraphs?*

Taking into account the aforementioned examples of risk assessment and prescreening measures in asylum and immigration law procedures, it is relevant to refer shortly to the proposal for a Regulation on Artificial Intelligence, presented by the Commission in April 2021.[42] The goal of the proposed regulation is amongst others to safeguard EU values and fundamental rights and to ensure the development of 'secure, trustworthy and ethical artificial intelligence'. The proposal provides general rules to be taken into account in the development and use of artificial intelligence (AI), but also explicitly defines specific 'harmful' AI to be prohibited (for example an AI based system of social scoring used by public authorities) and 'high risk AI systems'. The development and use of these 'high risk systems' are bound by stricter rules. It is noteworthy that the Commission, when describing examples of high-risk systems, explicitly refers to the possible use of 'polygraphs and similar tools or to detect the emotional state of a natural person' in the fields of migration, asylum and border control management.[43] Whereas any scientific evidence for the reliability of the use of polygraphs (read lie-detectors) is lacking (on the contrary, scientist have

39 See for the original text of the proposed Regulation on the establishment of Eurodac, COM (2020) 614, Articles 12 (v) which referred explicitly to the screening procedure in the proposed Screening Regulation.

40 See Council doc. 11873/21, 15 September 2021, pp 2 and 31.

41 See also the open letter to the European Parliament signed by different organisations, expressing their concerns about the fundamental rights impact of the new Eurodac proposal (Statewatch 8 September 2021) <https://www.statewatch.org/news/2021/september/eu-expanding-the-eurodac-database-meps-must-put-rights-first/> accessed 8 October 2021.

42 See (n 6).

43 See recital 39 and Article 6 of the proposed AI Regulation and point 7(a) of Annex III to this proposal, defining further high-risk AI systems. In the proposal, the Commission also

multiple times emphasized the flaws of these methods), this use of 'AI' entails severe risks for the protection of fundamental rights as it will increase the (already existing) problem of accountability, and result in further stigmatization of specific groups of individuals.[44] Therefore, it is worrying that instead of defining the use of polygraphs as a prohibited AI system, the AI proposal allows this use by national authorities and even by explicitly referring to its use in asylum, migration, and border control decisions. It is even more worrying, that the European Commission subsidizes research investigating the possible use of 'smart lie-detection system to tighten EU's busy borders'.[45]

4 Access to Effective Judicial Protection – Case Law by the CJEU

When discussing the applicable rules on legal remedies, two different legal regimes must be distinguished: first, legal remedies against the refusal of entry or a visa or travel authorisation itself, and second the right to appeal against the information upon which the denial of entry is based, the SIS alert or the risk assessment. As I will argue below, case-law by the CJEU dealing with refusals of short-term visa based on the Visa Code, provides relevant criteria to safeguard effective judicial protection, also within the framework of the use of 'soft' information, such as a risk assessment. Nevertheless, there are still important gaps with regard to the legal protection of TCNs which should be dealt with by the EU and national legislators.

refers to the use of polygraphs for law enforcement purposes. See also Niovi Vavoula in this special issue.

44 Petra Molnar, 'Technological Testing Grounds. Migration Management Experiments and Reflections from the Ground Up' (EDRi and the Refugee Lab 2020). See also Ryan Gallagher and Ludovica Jona, 'We tested Europe's new lie detector for travellers – and immediately triggered a false positive' (The Intercept, 26 July 2019) https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/.

45 <https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders> accessed 8 October 2021. This link provides information on a previous Horizon 2020 funded project 'iBorderctrl' investigating the use of lie-detection of travelers based on facial features during digital interviews with so-called 'border avatars'. The website of the research project iBorderctrl meanwhile disappeared. See for a new research project funded by the Commission, involving algorithm-based border controls: https://www.tresspass.eu/The-project.

4.1 *Access to Legal Remedies against the Refusal of Admission, Visa or Travel Authorisation*

Article 14 (3) of the Schengen Borders Code provides that persons refused entry have the right to appeal, which appeal will be conducted in accordance with national law. In accordance with Article 14 (2) the person must be provided with a substantiated decision stating the precise reasons for refusal, by means of the standard form as included in Annex VI to the Schengen Borders Code. This latter addition seems to undermine the rather strict requirement of the substantiated decision-making, as the standard form allows national authorities not to offer detailed information on the reasons for refusal. However, as discussed below, when dealing with CJEU's case-law, this standard form does not derogate from the general obligation of informed decision-making to ensure effective legal protection. Furthermore, in *E.P.*, the CJEU ruled on the question of how far the state's discretion reached regarding the evaluation of entry conditions.[46] The CJEU found that in the case of Article 6(1) of the Schengen Border Code, including the grounds to refuse a person entry to the Schengen area, the Member State had wide discretion in reaching the conclusion that an individual was a threat to public policy. In the same judgment, the CJEU, however underlined that any such decision must be based on a prior individual assessment and proportionality test. According to the CJEU, national practices on the return of TCNs 'must comply with the principle of proportionality, which is a general principle of EU law, and must therefore, in particular, not go beyond what is necessary to safeguard public policy'.[47] Furthermore, the CJEU stressed that national authorities may only invoke a threat to public policy if there is a 'consistent, objective and specific evidence that provides grounds for suspecting that that TCN has committed such an offence'.[48] These criteria, therefore, need to be effectively scrutinised by national courts.[49] Furthermore, as underlined by the CJEU with regard to the European Arrest Warrant and the SIS-alert for the refusal of entry, a state may have a duty to check the lawfulness of the (execution of) a SIS-alert, if this would violate fundamental rights, including the right to a fair trial and the freedom of movement of spouses of EU citizens of the person at stake.[50]

---

46 Case C-380/18 *E.P.*, EU:C:2019:1071, paras 47–49.

47 Ibid, para 47.

48 Ibid, para 49.

49 See also Pieter Boeles et al., 'Public Policy Restriction in EU Free Movement and Migration Law. General Principles and Guidelines' (Amsterdam 2021) <https://www.commissie-meijers.nl/sites/all/files/media/meijers_committee_-_public_order_in_eu_migration_law.pdf> accessed 8 October 2021.

50 Case C-404/15 *Aranyosi*, EU:C:2016:198; Case C-503/03 *Commission v Spain*, EU:C:2006:74.

Dealing with short-term visa applications, Article 32 (3) of the Visa Code provides that applicants 'who have been refused a visa shall have the right to appeal'.[51] Member States are required to disclose the grounds of the refusal to the applicant as provided in the standard form in Annex VI.[52] The form is divided in 11 reasons for refusal, annulment or revocation. Point 5 of the form addresses situations in which the refusal is based on an alert for the purpose of refusing entry issued by another Member State in the Schengen Information System.

In general, these provisions offer Member States much leeway with regard to both the decision-making in visa procedures and the scope and content of legal remedies. With regard to the former, the CJEU in *Koushkaki*, emphasized that the listed grounds for refusal in Article 32(1) of the Visa Code are exhaustive and therefore a visa refusal cannot be based on any other ground.[53] With regard to the latter, in the *El Hassani* case, the CJEU clarified that the, even if rather vague, the provision on the right to appeal in the Visa Code does not entail a discretionary power for Member States, by stressing the close relationship between Article 32 Visa Code and Article 47 of the EU Charter of Fundamental Rights (EU Charter) on the right to effective judicial protection.[54] According to the CJEU, where 'in examining a visa application the national authorities have a broad discretion as regards the conditions for applying the grounds of refusal laid down by the Visa Code and the evaluation of the relevant facts, the fact remains that such discretion has no influence on the fact that the authorities directly apply a provision of EU law.'[55] Therefore, Article 32(3) of the Visa Code, read in the light of Article 47 EU Charter, requires Member States 'to provide for an appeal procedure against decisions refusing visas, the procedural rules for which are a matter for the legal order of each Member State in accordance with the principles of equivalence and effectiveness.[56]

4.2 *Access to Legal Remedies in Relation with the Information Contained in EU Databases*

One of the keystones of data protection and the enforcement of data subjects' rights to access, correction or deletions of their data, is the right to effective

51 Case C-403/16 *El Hassani*, EU:C:2017:960.

52 Article 32(2) Visa Code.

53 Case C-84/12 *Koushkaki*, EU:C:2013:862, para 38. See also Steve Peers, Elspeth Guild and Jonathan Tomkin (eds) *EU immigration and asylum law, Volume 1 Visas and border controls* (Martinus Nijhoff 2012) 261.

54 *El Hassani* (n 51) paras 33–42.

55 Ibid, para 36.

56 Ibid, para 42.

judicial remedies.[57] Article 68 of the new SIS II Regulation maintains the same provision with regard to access to legal remedies as was already included in the Regulation 1987/2006. It allows data subjects to bring an action before any competent authority, including a court, under the law of any Member State with regard to their rights concerning the entry, rectification, completion, and deletion of their personal data in SIS II. This means that a data subject may proceed in any Member State regardless of whether this state submitted the SIS alert. If a national data protection authority or court finds that the data should be corrected or even deleted from the SIS II, this decision must be executed by the reporting state. This provision in the SIS II Regulation allows TCNs therefore to submit a request or lodge an appeal without having to find out first which states submitted the SIS alert. As we have seen above, this is different for a person whose visa application is rejected based on the objection of another Member State.

The Visa Information System or VIS includes information on every decision adopted with regard to a short-term visa application by a TCN on the basis of the Visa Code. Article 38 VIS Regulation[58] also includes an individual right to access, correction and deletion of information in the VIS database on short-stay visas and based on Article 40 a person refused this right, has the right to bring an action or a complaint before the competent authorities or courts of that Member State. Member States are thus not obliged to provide a remedy before courts. In accordance with Article 38 (6), a Member State must inform the person on how 'to bring an action or a complaint before the competent authorities or courts of that Member State' and on any assistance, including from the national data protection authorities. Whereas this obligation is an important safeguard for legal protection, it is unclear how it is implemented in practice.

With regard to the future use of ECRIS-TCN, Article 25 of the ECRIS-TCN Regulation provides that requests of TCNs for rectification and erasure and to restrict the processing of personal data, which rights are set out in the applicable Union data protection rules, may be addressed to the central authority of any Member State. Where a request is made to a Member State other than the convicting Member State, the former Member State shall forward it to the convicting Member State without 'undue delay' and in any event within 10 working days of receiving the request. Upon such request, the convicting

57 Case C-362/14 *Schrems*, EU:C:2015:650, para 95.

58 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) [2008] OJ L218.

Member State must immediately launch a procedure for checking the accuracy of the data concerned and the lawfulness of its processing in ECRIS-TCN; and respond to the Member State that forwarded the request without undue delay. If this convicting state does not agree that the data in ECRIS-TCN are inaccurate or have been processed unlawfully, it will adopt in accordance with Article 25 (4) an administrative or judicial decision explaining in writing to the person concerned why it is not prepared to rectify or erase data relating to him or her. Such cases may, where appropriate, be communicated to the national supervisory authority. Article 25 (5) obliges the Member State adopting the decision pursuant to paragraph 4 to provide the person concerned with information explaining the steps he or she can take if the explanation given pursuant to paragraph 4 is not acceptable to him or her. This includes information on how to bring an action or a complaint before the competent authorities or courts of that Member State and any assistance, including from the national supervisory authorities, that is available in accordance with the national law of that Member State. In case of such refusals the Member States must provide in accordance with Article 27 of the ECRIS-TCN Regulation, 'any person the right to lodge a complaint and the right to a legal remedy in the convicting Member State which refused the right of access to or the right of rectification or erasure of data relating to him or to her. Where Article 27 does not explicitly state whether this entails judicial remedies, we have learned from CJEU case-law that applicable provisions on legal remedies must be read in accordance with Article 47 of the Charter.[59] This means that Member State must ensure access to effective judicial protection for individuals lodging an appeal against decisions refusing to correct or delete information in ECRIS-TCN. Contrary to the provision in the aforementioned SIS II Regulation, the right to a legal remedy in the ECRIS-TCN Regulation does not allow the individual to start proceedings in any of the Member States using ECRIS-TCN. As a result, this person may have to start procedures in different states: one in the state refusing entry on the basis of the ECRIS-TCN information, and one in the convicting. This may hamper his or her right to have access to effective judicial protection.

4.3 *Access to Legal Remedies with Regard to 'Risk Assessments'*

In accordance with Article 37 (3) of the ETIAS Regulation,[60] an applicant who has been refused a travel authorisation shall have the right to appeal. Such appeal must be conducted in the Member State that has taken the decision on the application and in accordance with the national law of that Member

59 See the aforementioned *El Hassani* (n 51) and in the context of the Dublin Regulation, Case C-63/15 *Ghezelbash*, EU:C:2016:409.

60 n 30.

State. The ETIAS National Unit of this Member State responsible must provide the applicants with information regarding the appeal procedure. If an application for travel authorisation is refused, Article 38 of the ETIAS Regulation provides that the applicant should receive a notification by email. This notification must include information on the right to appeal and a statement of the grounds of refusal as listed in Article 37 (1) and (2). These refusal decisions will not include substantiated or individualised information; they merely state the category of the grounds of refusal (such as, the fact that the person is reported in the SIS for the purpose of refusal of entry, or that s/he poses a security, illegal immigration, or high epidemic risk).

Neither the Screening proposal, nor the proposed Regulation on Asylum and Migration Management[61] provide any legal remedy against the assessment that a person poses a security risk, or any obligation for authorities to inform the TCN about this assessment or 'security flag'. Second, the proposed Screening Regulation does not seem to provide a legal remedy against a refusal of entry based on the screening procedure within the framework of search and rescue operations, as these operations are excluded from the applicability of the Schengen Border Code.[62] Furthermore, when dealing with the decision whether a person falls within one of the four aforementioned categories, there is no appeal right for an individual who submits that he or she has been wrongly categorized. This might be particularly problematic where at the external borders or during safe and rescue operations, individuals due to misunderstanding or lack of information, are wrongly categorized as not applying for asylum.

A comparable problem applies to individuals whose application for entry, a visa or travel authorisation, or asylum, is rejected based on the use of risk assessment, artificial intelligence, or even polygraphs. Currently, EU legislation does not provide in extra guarantees with regard to the right to appeal against such decision-making.

4.4 *Effective Remedies ... with a Little Help from the CJEU*

As we have seen above, where the refusal of admission is based on foreign information as is the case in the framework of the SIS, the consultation mechanism in the visa procedure, and in ECRIS-TCN, TCNs will be hampered to address this decision-making effectively.

61 Proposal for a Regulation of the European Parliament and of the Council on asylum and migration management and amending Council Directive (EC) 2003/109 and the proposed Regulation (EU) XXX/XXX [Asylum and Migration Fund], COM/2020/610 final.

62 See, Article 14 (1) of the Screening proposal.

In the case *R.N.N.S and K.A* the CJEU provided relevant guidelines to ensure access to effective judicial protection in cases where two states are involved in the denial of entrance.[63] In this case, the Dutch visa authorities had refused a short-term visa to TCNs following objections from Hungary, respectively Germany.[64] Moreover, the Dutch authorities did not provide information on the reasons for refusal and claimed they had no discretion to issue a visa related to the objection of another state.[65] In both cases, the applicants were referred to the objecting states with regard to their right to appeal under Article 32 of the Visa Code. However, due to the absence of a formal decision, it was difficult if not impossible for the applicants to lodge legal proceedings in the respective states. In both cases, also because of the use of the standard form provided in Annex VI of the Visa Code, the visa refusal itself did not offer the applicants clear or precise information on the grounds of refusal, and at first, not even about which state objected against the issuing of a visa.

In *R.N.N.S. and K.A.*, the CJEU states that despite 'the broad discretion as regards the conditions for applying the grounds for refusal', such discretion has no influence on the fact that they directly apply a provision of EU law.[66] 'This means that in accordance with Article 47 (2) of the EU Charter, applicants are entitled to a hearing by an independent and impartial tribunal. Furthermore, compliance with that right assumes that a decision of an administrative authority 'that does not itself satisfy the conditions of independence and impartiality must be subject to subsequent control by a judicial body that must, in particular, have jurisdiction to consider all the relevant issues'.[67] Whereas the definition of 'all the relevant issues' can be considered vague, it does provide an important criterion for the scope of judicial review of

63 Joined Cases *R.N.N.S and K.A.* C-225/19 and C-226/19, EU:C:2020:951.

64 District Court Den Haag zp Haarlem, 31 July 2018, AWB 17/15895 and AWB 18/7781, 24 November 2020. The first case concerned the visa application of an Egyptian national with a Dutch spouse, who want to visit his parents in law in the Netherlands and whose application was rejected on the basis of the objection from Hungary. The second case concerned the visa application of a Syrian national living in Saudi Arabia, who wanted to visit his children in the Netherlands but whose visa was refused based on a German objection.

65 In the first case, when the applicant's lawyer found out the objecting state concerned Hungary, and approached the Hungarian authorities to find out about possible ways of legal redress, she was informed there was no legal address due to a failure of a formal decision. Which meant that the fact of informing the Netherlands about the objection, was not considered as a formal decision.

66 *R.N.N.S and K.A*, para 36.

67 Point 39, where the CJEU also refers to the earlier *Berlioz Investment Fund* judgment (C-682/15).

the decision-making in visa procedures. In connection with earlier judgment of the CJEU in *EP*, addressing the prohibition of automated decision making and the necessity of an individual assessment, this means that national courts must be able to address in the visa application the specific reasons and legitimacy of the decision at stake.

Furthermore, the CJEU emphasized that to ensure that the right to judicial protection is effective, the person concerned must be able to ascertain the reasons upon which the decision taken in relation to him or her is based, either by reading the decision itself, or by requesting and obtaining notification of those reasons.[68] With regard to the role of the courts, the CJEU made a distinction between on the one hand the review by courts of the Member State which adopted the final decision of refusing a visa, which concerns the examination of the legality of that decision, and on the other hand the review of the merits of the objection to the issuing of a visa raised by another Member State. The CJEU emphasized the obligation of the Member State refusing a visa, to ensure that the rights of defence and the right to a remedy of the visa applicant are guaranteed. This includes the obligation to indicate in the visa refusal decision, the identity of the Member State which raised that objection, the specific ground for refusal on the basis of that objection, and, 'where appropriate', the essence of the reasons for that objection.

It may be considered disappointing that the CJEU in this judgment explicitly found that the courts of the Member State adopting the final decision, cannot examine the substantive legality of the objection raised by another Member State to the issuing of the visa. The CJEU could have chosen for a parallel reasoning with the provision in the SIS II Regulation. As discussed above, this allows TCNs to seek legal remedies in any of the Member States and provides national courts and tribunals the power to order national authorities from other states to delete or correct SIS alerts, or to grant compensation for harm caused by the use of SIS. However, in *R.N.N.S. and K.A.*, the CJEU did rule that to enable the visa applicant to exercise in accordance with Article 47 EU Charter his or her right to challenge such an objection, the Member State refusing a visa, should provide information on the authority the applicant may contact in order 'to ascertain the remedies available in that other Member State'.[69] It should be noted that the CJEU added an apparently superfluous, but meaningful remark: 'in any event, the Member State concerned may issue a visa with limited territorial validity in accordance with Article 25 of the Visa

68 *R.N.N.S. and K.A.*, paras 43–56.
69 Ibid, para 52.

Code'.[70] The CJEU made this statement after describing all the necessary safeguards to be adopted by the Member State taking the final decision of refusal to ensure effective judicial protection. This could be read as a gentle instruction to individual states that where there are insufficient (substantiated) grounds for refusing entry, the Member State should grant the applicant in any case access to its own territory, thus providing an implicit exception to mutual trust.

5 Conclusions

In the proposed EU Migration and Asylum Pact, the European Commission calls for a 'robust and fair management of external borders, including identity, health and security checks.'[71] At this moment, the EU legislator is developing new tools of exclusion which, together with existing tools such as the use of SIS, raise several questions with regard to both their robustness and fairness. As emphasized by Leese and others, border control thus 'has become a practice of data-driven knowledge production that serves to facilitate processes of social sorting, risk assessment, and prevention'.[72] Whereas the necessity of several measures, such as the use of ECRIS-TCN for the purpose of immigration control, is insufficiently substantiated, the risk of the combined and automated use of such 'exclusion tools' is too high for the legal protection of the individuals concerned.

Individuals who have been denied entry, a visa, or travel authorisation for the Schengen area should always be informed about which record in which information system exists, and subsequently resulted in a refusal. The same holds for decisions based on the objection from another state and exclusion based on risk assessment or a 'security flag'. Whereas such guarantees are currently lacking, this gap should be repaired during future negotiations dealing with the relevant legislation.[73] At the same time, the use of 'polygraphs' or any form of lie-detectors within the framework of asylum and immigration decision-making should be explicitly prohibited.

Addressing in particular the ETIAS Regulation, the European Data Protection Supervisor (EDPS) stressed rightfully that an applicant should receive sufficiently clear indication of the ground(s) for refusal in order to

70 Ibid, para 55.

71 Communication from the Commission on a New Pact on Migration and Asylum, COM (2020) 609 final, 23 September 2020, p 2.

72 Matthias Leese, Simon Noori and Stephan Scheel, 'Data Matters: The Politics and Practices of Digital Border and Migration Management' (2021) Geopolitics 2.

73 See also Vavoula (n 29) 48 and 54.

efficiently exercise his or her appeal and contest the reasons for the refusal. Furthermore, the law at stake should specify the information to be provided to rejected applicants, especially where a refusal would be based on a hit with any other data system.[74] This guarantee should specifically apply, also in the context of the use of other databases discussed above, where decisions are based on information from third states.

The complexity of legal instruments at stake (in combination with further use of personal information via the interoperability scheme) hamper the effective use of individual data protection rights and judicial remedies as protected in Article 47 of the EU Charter.[75] The involvement of different Member States and actors in the decision-making on who is allowed entrance and who is not, makes it further difficult if not impossible for TCNs to address the responsible authorities. In addition, the flagging of persons who are identified as security risk during the screening procedure and AI based risk assessments, will cause a huge impact for the individual rights and mobility of TCNs. An important role is left for the national courts ensuring close scrutiny of these measures, but in the first place it is the legislator who should fill in the current gaps with regard to the right to an effective remedy.

74 EDPS, 'Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS)' (Opinion 3/2017) 17–18 <https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_en.pdf> accessed 8 October 2021.

75 See my and the other contributions in the special issue on interoperability in (2020) 26(1) European Public Law.