BRILL
NIJHOFF

EUROPEAN JOURNAL OF MIGRATION
AND LAW 22 (2020) 139–177

European
Journal of
Migration
and Law

brill.com/emil

Consultation of EU Immigration Databases for Law Enforcement Purposes: a Privacy and Data Protection Assessment

Niovi Vavoula
Lecturer in Migration and Security, Queen Mary University of London, London, UK
n.vavoula@qmul.ac.uk

Abstract

Since the past three decades, an elaborate framework of EU-wide information systems processing the personal data of third-country nationals has emerged. The vast majority of these systems (VIS, Eurodac, EES, ETIAS) are conceptualised as multi-purpose tools, whereby their consultation for crime-related objectives is listed among their ancillary objectives. As a result, immigration records may be accessed by national law enforcement authorities and Europol for the purposes of fighting terrorism and other serious crimes under specified and limited conditions. Drawing from the relevant jurisprudence of the European Court, this article evaluates whether the EU rules on law enforcement access to EU immigration databases comply with the rights to respect for private life and protection of personal data, as enshrined in Article 7 and 8 of the EU Charter respectively. In addition, challenges posed by the forthcoming interoperability between databases are also examined.

Keywords

databases – Eurodac – VIS – EES – ETIAS – interoperability – law enforcement – privacy

1 Introduction

In an era of globalised crime, the evolution of digital technologies has opened up new possibilities for the use of personal data in the law enforcement context. At EU level, efforts to facilitate the flow of personal data have translated to two

 | DOI:10.1163/15718166-12340072

main strands of legislative action; the proliferation of legal channels of information exchange among national and EU bodies, with progressive expansion outside the EU,[1] and the maximisation of access by law enforcement authorities to information systems for immigration control, despite the undoubtedly different objectives of managing migration and combating crime. These initiatives involve a 'mille-feuille' of information processing schemes, currently comprising three operational databases—the Schengen Information System (SIS II, formerly SIS), Eurodac and the Visa Information System (VIS)—and three on paper—the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the European Criminal Record Information System for third-country nationals (ECRIS-TCN).[2] Largely justified by counter-terrorism concerns[3]—both in the aftermath of 9/11[4] and in recent years[5]—these databases are accessed by national law enforcement authorities and Europol, although they primarily serve purposes linked to border and immigration control. This takes place either because of the law enforcement mandate (SIS II and ECRIS-TCN), or because consultation of immigration data in the fights against terrorism and other serious crimes is included among the ancillary objectives of certain databases, thus enabling access by national law enforcement authorities and Europol to the data stored under specific conditions enshrined in the legal instruments regulating their operation (Eurodac, VIS, EES and ETIAS).

This latter case of databases that are used as criminal law tools on an ancillary basis is examined by the present article with the aim to assess whether the modalities of access comply with the rights to respect for private life and protection of personal data, as enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights (EU Charter) and Article 8 of the European Convention on Human Rights (ECHR). Emphasis in that respect is placed on whether the EU rules are necessary and *stricto sensu* proportionate and the approach taken regarding the relationship between the rights to private life and personal data protection is the one taken by the European courts.[6] To that

1 Mitsilegas, V. (2009). *EU Criminal Law*. Oxford and Portland: Hart, ch. 5.

2 For a detailed analysis on databases for third-country nationals see Vavoula, N. (forthcoming 2020). *Immigration and Privacy in the Law of the European Union: The Case of Databases*. Leiden: Brill Nijhoff.

3 See Mitsilegas, V. (2005). Contrôle des Étrangers, des Passagers, des Citoyens: Surveillance et Anti-Terrorisme. *Cultures et Conflits* 58, pp. 185–197.

4 For example, see the Declaration on Combating Terrorism (25.03.2004), p. 7.

5 For example, see the European Agenda on Security (COM(2015) 185 final) as well as the numerous Progress Reports that unwrap it.

6 See below Section 4.

end, a compact outline of the existing and forthcoming information systems is provided, with emphasis on the provisions according to which national law enforcement bodies and Europol may access immigration data (Sections 2 and 3). The collection and further processing of personal data of different groups of third-country nationals through centralised databases primarily constitutes an interference with the rights to private life and protection of personal data. Though legal scholars have examined the operation of databases in the context of immigration control from the perspective of fundamental rights,[7] access to their data for law enforcement purposes has so far attracted limited scholarly attention.[8] Furthermore, an analysis comparing the rules on law enforcement access of all relevant databases, including how these rules are revised in view of the forthcoming interoperability of EU information systems remains elusive. For the purposes of this article, primary materials, such as evaluation reports and Council documents, are employed to argue that the arguments supporting law enforcement access have not been convincing and *ex-post* evidence of effectiveness of this function remains limited. The author further suggests that law enforcement access as a policy choice reflects an understanding of third-country nationals as security risks (Section 4.1). As for the proportionality assessment, the article draws from the jurisprudence of the European courts; although to date immigration databases have not generated case law, the CJEU's pronouncements in other cases concerning the use of personal data collected for other purposes than those for which they have been originally collected for, particularly *Digital Rights Ireland*,[9] *Tele2 and Watson*,[10] *Opinion 1/15*[11] provide useful pointers for this analysis. The findings of the ECtHR in cases such as *Zakharov v Russia*,[12] also provide a benchmark to assess the proportionality of the modalities of access. In that regard, the article uses the criteria that have been employed by the European courts to assess the conditions that law enforcement bodies and Europol must fulfill in

7 For example, for a detailed overview of the SIS see Brouwer, E. (2008). *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*. Leiden: Martinus Nijhoff.

8 See Mitsilegas, V. (2009). The Border Paradox: The Surveillance of Movement in a Union without Internal Frontiers, in: H. Lindahl (Ed.), *A Right to Inclusion and Exclusion? Normative Fault Lines of the EU's Area of Freedom, Security and Justice*. Oxford and Portland: Hart, pp. 33–63.

9 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Ireland*, ECLI:EU:C:2014:238.

10 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v. Post-och Telestyrelsen, and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, ECLI:EU:C:2016:970.

11 Opinion 1/15, ECLI:EU:C:2017:592.

12 *Zakharov v Russia* (2015) ECHR 1065.

order to access the data stored, the offences in relation to which such access is allowed, the authorities that may process the data and the data that are consulted. In following the Courts' approach, principles of EU data protection law, such as purpose limitation and data quality, are also referred to—albeit to a more limited extent—as these principles though not featured in the case law, reinforce the author's arguments in assessing necessity and proportionality of law enforcement access to immigration databases. Finally, the reforms to the procedure stemming from the forthcoming interoperability among EU information systems are also critically discussed (Section 5).

2 EU Databases for Third-Country Nationals: a Sketch

Since the past three decades, an elaborate framework of large-scale information systems has emerged, whereby a wide array of personal data, including biometrics, collected by different categories of third-country nationals are stored and further processed for a wide range of purposes. Indeed, the flexible and dynamic nature of databases that enables adaptability to the evolving digital technologies and perceived threats to the EU has meant that the systems may be used for different objectives spanning from modernising immigration control to law enforcement.

2.1 *The Security Tool: SIS II*

Perhaps the best-known database is the SIS II, the purpose of which is to maintain a high level of security within the Schengen Area.[13] At the heart of the compensatory measures for the abolition of internal border controls, the SIS II registers 'alerts' on various categories of persons and objects, for example, people wanted for arrest for extradition, or persons or objects subject to discreet, inquiry or specific checks.[14] In addition, it stores alerts on third-country nationals to be refused entry into or stay in the Schengen area,[15] or are subject to return proceedings.[16] Hence, by its hybrid nature, the SIS II serves as both immigration and criminal law instrument. In connection to each alert, the SIS II stores basic alphanumeric information, as well as biometric data (fingerprints, photographs, palm prints and DNA files)[17] and is complemented

13 The legal bases of the SIS II are: Regulation (EU) 2018/1860 [2018] OJ L312/1; Regulation (EU) 2018/1861 [2018] OJ L312/14; Regulation (EU) 2018/1862 [2018] OJ L312/56.

14 For the alerts see Regulation 2018/1862, arts. 26–41.

15 Regulation 2018/1861, arts. 20–31.

16 Regulation 2018/1860, art. 3.

17 Regulation 2018/1862, arts. 42–43.

by SIRENE that enables searches for supplementary information in cases of a 'hit'.

2.2 *The Multifunctional Tool: VIS*

The VIS was conceptualised in the aftermath of the 9/11 events[18] to modernise the administration, issuance and checks of short-stay visas by enabling the exchange of personal data on visa applicants.[19] Its overarching aim is to assist in the development of the common visa policy, however, no less than seven wide-ranging sub-purposes are set out, among which is the prevention of threats to the internal security of the EU Member States.[20] To that end, a separate instrument has been adopted, Decision 2008633/JHA (VIS Decision),[21] that lays down the modalities by which visa data may be consulted by law enforcement authorities and Europol. Overall, the system stores a broad range of personal data, including fingerprints and photographs of all persons subject to visa requirements, irrespective of the status of their visa application.[22]

2.3 *The Dublin Tool: Eurodac*

Eurodac[23] aims at assisting in the implementation of the Dublin system on the allocation of the Member State responsible for examining an application for international protection.[24] To that end, the system processes the fingerprints

18 Baldaccini, A. (2008). Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases. *European Journal of Migration and Law* 10(1), pp. 31–49.

19 Council Decision 2004/512/EC [2004] OJ L213/5; Regulation (EC) 767/2008 [2008] OJ L218/60, as amended by Regulation (EC) 810/2009 [2009] OJ L243/1 (VIS Regulation).

20 These are: a) Facilitating the visa application procedure; b) Preventing 'visa shopping'; c) Facilitating the fight against fraud; d) Facilitating checks at external border crossing points and within national territory; e) Assisting in the identification of persons that do not meet the requirements for entering, staying or residing in a Member State; f) Facilitating the implementation of the Dublin mechanism; and g) Contributing to the prevention of threats to Member States' internal security. On the ranking of these purposes by the CJEU, see below.

21 Council Decision 2008/633/JHA [2008] OJ L218/129 (VIS Decision). The need for a separate EU instrument is attributed to the then pillar structure. A bridging clause (art. 3) links the Regulation with the Decision.

22 VIS Regulation, art. 9. A reform of the VIS legal basis is currently negotiated, so that the personal scope of the database will cover holders of residence permits, residence cards and long-stay visas. See COM(2018) 302 final.

23 It was created by Council Regulation 2725/2000 [2000] OJ L316/1 and Council Regulation 407/2002 [2002] OJ L62/1. The latest legal basis is Regulation 603/2013 [2013] OJ L180/1 (recast Eurodac Regulation).

24 Dublin Convention [1997] OJ C254/1, replaced by Regulation 343/2003 [2003] OJ L50/1 (Dublin II Regulation) and Regulation (EU) 604/2013 [2013] OJ L180/31 (Dublin III Regulation).

of all asylum seekers over the age of fourteen,[25] as well as those persons found irregularly crossing the external borders or staying on national territory,[26] to check whether these have already been recorded by another Member State.[27] If a Eurodac check reveals that the fingerprints have already been recorded, the individual may be sent to that Member State.[28] A year after the database had begun its operation, the 2004 Hague Programme called for the maximisation of effectiveness of EU information systems and 'an innovative approach to the cross-border exchange of law enforcement information'.[29] Almost a decade afterwards, after four proposals and largely under the pressure of finalising the second phase of the Common European Asylum System (CEAS),[30] Regulation 603/3013 was adopted in June 2013,[31] opening up the database to national law enforcement authorities and Europol.[32]

2.4 *The Schengen Hotel: EES*

Influenced by similar initiatives in the US, in 2013 the Commission presented the so-called 'Smart Borders Package', including a proposal to establish an Entry/Exit System (EES) that will record border crossing both at entry and exit of third-country nationals admitted for a short stay.[33] Due to proportionality and budgetary concerns,[34] the Commission originally left the registration of

25 Recast Eurodac Regulation, arts. 9–13.

26 Recast Eurodac Regulation, arts. 14–17. However, the fingerprints of migrants found irregularly staying are not centrally stored, but only compared with existing records.

27 A Eurodac reform is underway that expands the personal and material scope of the database: by requiring the registration of records on irregular stayers, by increasing the categories of personal data collected, by modifying the storage period, by lowering the fingerprinting obligation to encompass children over the age of six and by adding photos. See COM(2016) 272 final.

28 For an analysis see Guild, E. (2007). Unreadable Papers? The EU's First Experiences with Biometrics: Examining Eurodac and the EU's Borders, in: J. Lodge (Ed.), *Are You Who You Say You Are? The EU and Biometric Borders.* Nijmegen: Wolf Legal Publishers, pp. 31–43.

29 The Hague Programme [2004] OJ C53/1, p. 7.

30 B. Juster and V. Tsianos (2013). Erase Them! Eurodac and Digital Deportability, *Transversal/EIPCP Multilingual Webjournal*, February, https://transversal.at/transversal/0313/kuster-tsianos/en accessed 27 August 2019.

31 See n 23.

32 Law enforcement access to Eurodac data is enabled since 2015. Denmark, Iceland, Liechtenstein, Norway and Switzerland do not apply any of the law enforcement related provisions though and protocols are required.

33 COM(2013) 95 final. The other proposals involved a 'Registered Travellers Programme' (COM(2013) 97 final) and amendments to the Schengen Borders Code (COM(2013) 96 final).

34 For criticism, see among others EDPS [2014] OJ C32/25 (executive summary); Article 29 Data Protection Working Party, Opinion 05/2013 on Smart Borders (WP206, 2013); Standing

biometrics and law enforcement access outside the scope of the proposal and later the package was entirely withdrawn. However, in the aftermath of the 2015 terrorist events, the EES was adopted in November 2017.[35] The EES is also a multi-purpose tool: it will enhance the efficiency and automation of border checks; assist in the identification of irregular migrants and overstayers; combat identity fraud and misuse of travel documents; and strengthen internal security by allowing law enforcement authorities access to travel history records.[36] To those ends, it will record the identities of third-country nationals, by storing alphanumeric data, four fingerprints and a facial image, along with details of their travel documents, which will be linked to electronic entry and exit records.[37] As a result, the Schengen area will function as a 'Schengen hotel', whereby third-country nationals entering into it and exiting from it will be required to check-in and check-out respectively.

2.5 *The Screening Test: ETIAS*

The ETIAS will also be concerned with visa-free travellers, with emphasis on their pre-vetting prior to their entry in the Schengen area. The ETIAS Regulation, enacted in September 2018,[38] solidifies the link between immigration control and security, as one of its main objectives is to contribute to a high level of security by thoroughly assessing whether travellers pose a 'security risk'.[39] The database is therefore a pre-emptive control mechanism that also serves many other purposes, including the prevention of irregular migration and the contribution to the prevention, detection and investigation of terrorist offences and other serious offences.[40] To achieve these aims, all visa-exempt travellers shall be obliged to obtain authorisation prior to their departure by disclosing a series of personal data.[41] A pre-screening procedure shall take place on the basis of cross-checking against databases, certain screening rules on the basis of risk indicators;[42] and a special ETIAS watch list of individuals suspected of terrorism or other serious crimes.[43]

Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), Note on the Smart Borders proposals (COM(2013) 95 final, COM(2013) 96 final and COM(2013) 97 final) (CM1307, 2013).

35 Regulation (EU) 2017/2226 [2017] OJ L32720 (EES Regulation).

36 Regulation 2017/2226, art. 6(1).

37 Regulation 2017/2226, arts. 14–20.

38 Regulation (EU) 2018/1240 [2018] OJ L61/1 (ETIAS Regulation).

39 Regulation 2018/1240, art. 4(a).

40 Regulation 2018/1240, art. 4(b)–(f).

41 Regulation 2018/1240, art. 17.

42 Regulation 2018/1240, art. 33.

43 Regulation 2018/1240, art. 34.

2.6 *The Judicial Cooperation Tool That May Be Used for Immigration Purposes: ECRIS-TCN*

The latest member in the databases' family is the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).[44] The latter emerged as a necessity in the law enforcement context, as in order to obtain complete information on previous convictions of third-country nationals, States were obliged to send 'blanket requests' to all other Member States. The ECRIS-TCN will be a centralised system for the exchange of criminal records on convicted third-country nationals and stateless persons, including dual nationals, and is meant to complement the already existing, decentralised ECRIS system through which information on the criminal records of EU nationals is exchanged. A novelty of ECRIS-TCN is that in accordance with Article 7(1) of the ECRIS-TCN Regulation, the database that was primarily set up in the context of judicial cooperation may be used for immigration control purposes if allowed and in accordance with national laws.

3 Access to Immigration Data by National Law Enforcement Authorities and Europol Circumscribed by Limited Conditions: an Ancillary Objective

In the light of the above, the VIS, Eurodac, EES and ETIAS may be accessed by national law enforcement authorities and Europol. As shown below in the comparative table, such access takes place under specific—albeit different—conditions. The databases are conceived and designed as multi-purpose tools serving a series of (divergent) objectives, thereby heavily blurring the boundaries between immigration and criminal law. Conversely, the ECRIS-TCN prescribes immigration use of criminal law data under conditions, which are however laid down under national law and no EU rules are foreseen. As for the SIS, access by domestic law enforcement authorities and Europol is restricted in terms of the purpose for which the processing of records may take place.

Consultation of immigration data for law enforcement purposes is merely an ancillary objective and thus exceptional in nature. This has been clarified by the CJEU in a case that arose in relation to the VIS.[45] The UK, which pursuant to its opt-out privileges does not form part of it—since this constitutes a development of the Schengen *acquis* to which it did not participate—, sought annulment of the VIS Decision on the grounds that it constitutes a police

44 Regulation (EU) 2019/816 [2019] OJ L135/1 (ECRIS-TCN Regulation); Directive 2019/884 [2019] OJ L151/143.

45 Case C-482/08 *UK v Council* [2010] OJ I-10413.

cooperation measure. The Court rejected the UK submission and upheld the VIS Decision basing its reasoning on the effectiveness and the special nature of Schengen cooperation. Although it contended that the aim of the VIS Decision falls within the sector of police cooperation, it opined that the content is related to both the common visa policy and police cooperation.[46] In particular, the Court observed that

> [The VIS Decision] provisions nevertheless contain conditions restricting access to the VIS [...] which make clear that they organise in essence the ancillary use of a database concerning visas, the principal purpose of which is linked to the control of borders and of entry to the territory and which is therefore available, merely by way of consultation, for police cooperation purposes on a secondary basis only, solely to the extent that use for those purposes does not call into question its principal use.[47]

The judgment thus stressed that the use of the VIS in law enforcement context has to be treated as secondary and collateral. In order to justify this view, the Court took note of the specific conditions of law enforcement access that testify for its exceptional character. Therefore, opening up the VIS to criminal law agencies and Europol is an add-on, which is by default beyond the original purpose of the database and that is why it is necessary to specify the rules and procedures of access in a limited manner. This corresponds to what Advocate General Mengozzi mentioned in his opinion, that the VIS itself does not have a function linked to the prevention and punishment of crimes, thus the specific access should be treated as exceptional and limited.[48]

The aforementioned proclamations are also relevant to the cases of Eurodac, EES and the ETIAS, which may also be consulted by national law enforcement authorities and Europol under specific conditions. Despite any variations, the significant deviation from their original immigration context is reflected in that law enforcement access is subject to a series of limitations, tailor-made to the specificities of each database with a key limitation being that consultation of immigration data is only reserved to cases involving the prevention, detection or investigation of terrorist offences and other serious crimes.

For the purposes of this article, a comparative table illustrating the modalities of law enforcement access to databases by national bodies and Europol is hereby provided, the design of which corresponds to the chronological order in which each legal instrument was adopted.

46 *Ibid.*, paras 50–51.

47 *Ibid.*, para. 52.

48 Case C-482/08 *UK v Council* [2010] OJ I-10413, Opinion of AG Mengozzi, para. 10.

TABLE 1 Modalities of access to immigration control databases by national law enforcement authorities and Europol

A. National law enforcement authorities

	VIS (VIS Decision)	Eurodac (Recast Eurodac Regulation)
Authorities	– Designated authorities (art 3(1)) – (One or more) Central Access Point(s) (art 3(3))	– Designated authorities, except for agencies or units exclusively responsible for intelligence relating to national security (art 5(1)) – Verifying authority is (one or more) national authority(ies) or a unit of an authority (art 6(1)) – National Access Point(s)
Offences	Terrorist offences and serious crimes (art 2(c) and (d))	Terrorist offences and serious crimes punishable by a custodial sentence or a detention order for a maximum period of at least three years (art 2(1)(j) and (k))
Conditions of access	Art 5(1) 1. Access must be necessary for the prevention, detection or investigation of terrorist offences and other serious crimes; 2. Specific case; 3. Reasonable grounds to consider that consultation will substantially contribute to the prevention, detection or investigation of any criminal offence within the scope of access.	Art 20(1) 1. Prior comparisons with national fingerprint databases and the automated fingerprinting identification systems (AFIS) of all Member States unless there are reasonable grounds to believe that such comparison will not lead to identification; 2. Access must be necessary for the prevention, detection or investigation of terrorist offences and other serious crimes, which means that there is an overriding public security concern, which makes the searching of the database proportionate; 3. Specific case (no systematic comparisons); 4. Reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any criminal offence within the scope of access, in particular when there is substantiated suspicion that the suspect, perpetrator or victim falls under the category covered by the recast Eurodac Regulation.

EES (EES Regulation)	ETIAS (ETIAS Regulation)
– Designated authorities (art 29(1)–(2)) – (One or more) Central Access Point(s) (art 29(3)–(4))	– Designated authorities (art 50(1)) – (One or more) Central Access Point(s) (art 50(2))
Same as Eurodac (art 3(1)(24)–(25))	Same as Eurodac (art 3(1)(15)–(16))
Art 32 1. Access must necessary for the purpose of prevention, detection or investigation of a terrorist offence and other serious crimes; 2. Specific case; 3. Evidence or reasonable grounds to consider that the consultation will contribute to the prevention, detection or investigation of a criminal offence, in particular when there is substantiated suspicion that the suspect, perpetrator or victim falls under the category covered by the EES Regulation; 4. Prior search has been conducted in national databases; 5. For searches with fingerprints a prior search must have launched in the Member States' AFIS. Conditions (4) and (5) do not apply when there are reasonable grounds to believe that a comparison with the systems of the other Member States will not lead to the verification of the identity or in cases of urgency.	Art 51(1) 1. Access must be necessary for the purpose of prevention, detection or investigation of a terrorist offence or another serious crime; 2. Specific case; 3. Evidence or reasonable grounds to consider that the consultation will contribute to the prevention, detection or investigation of a criminal offence, in particular when there is substantiated suspicion that the suspect, perpetrator or victim falls under the category covered by the ETIAS Regulation

TABLE 1 Modalities of access to immigration control databases (*cont.*)

	VIS (VIS Decision)	Eurodac (Recast Eurodac Regulation)
Procedure	– Reasoned written or electronic request by a designated authority; – Verification that the conditions of access have been fulfilled (art 4(1)) – In exceptional cases of urgency, oral requests are also acceptable and verification will take place *ex-post* (art 4(2))	– Reasoned electronic request – Verification that the conditions of access have been fulfilled – Transmission of the request by the verifying authority to the National Access Point (art 19(1)) – In exceptional cases of urgency where there is a need to prevent an imminent danger associated with a terrorist offence or other serious criminal offence the verification will take place ex-post (art 19(3))
Transfer to third countries or an international organisation	Prohibited, unless in an exceptional case of urgency, subject to the consent of the Member State that entered the data into the VIS (art 8(4)).	Prohibited. This prohibition shall also apply if those data are further processed at national level or between Member States (art 35(1)). Personal data which originated in a Member State and are exchanged between Member States following a 'hit' shall not be transferred if there is a serious risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of their fundamental rights (art 35(2)).

EES (EES Regulation)	ETIAS (ETIAS Regulation)
The standard procedure is the same as the VIS (art 31(1)) – In a case of urgency, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious crime, verification of the conditions of access may take place *ex-post* (art 31(2))	Same as the EES (art 51)
Prohibited. This prohibition shall also apply if those data are further processed at national level or between Member States (art 41(1)). – Derogation: in an exceptional case of urgency subject to the following conditions; a) the transfer must be necessary for the prevention, detection or investigation in the territory of the Member States or in the third country concerned; b) the designated authority has access to the data; the transfer is carried out in accordance with the Directive 2016/680; a duly motivated request has been submitted; the reciprocal provisions of any information of entry/exit records held by the requesting third country to the Member States operating the EES is ensured (art 41(6)).	Same as the EES (art 65(2) and (5)).

TABLE 1 Modalities of access to immigration control databases (*cont.*)

B. Europol

	VIS	Eurodac	EES	ETIAS
Conditions	Within the limits of Europol's mandate and where necessary for the performance of its tasks and for the purposes of a specific analysis or an analysis of a general nature and of a strategic type, provided that VIS data is rendered anonymous (art 7).	Within the limits of Europol's mandate and where necessary for the performance of its tasks; Conditions: 1. Prior comparisons against data stored in systems accessible by Europol must have not led to the identification of the data subject; 2. Comparison must be necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences, which means that there is an overriding public security concern which makes the searching of the database proportionate; 3. Specific case; 4. There must be reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of the criminal offence in question falls in the categories covered by Eurodac (art 21).	1. Consultation must be necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious crimes within Europol's mandate; 2. Specific case; 3. There must be evidence or reasonable grounds to consider that consultation will contribute to the prevention, detection or investigation of the offences at stake, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of an offence falls under the category covered by the EES Regulation (art 33(1)). – Access to the EES to identify an unknown suspect, perpetrator or suspected victim is allowed under the same conditions and if prior consultation of databases accessible by Europol has not made it possible to identity the person in question (art 33(2)).	Same as the EES, with the added condition that consultation must take place solely on the basis of specific search keys (art 53)

In a nutshell, the table illustrates that a specific process is foreseen according to which national law enforcement authorities, not always excluding intelligence agencies, and Europol consult data stored. Despite any variations on the entities involved, this process requires the requesting authority to manifest *ex ante* the fulfillment of specific conditions justifying the necessity of accessing the records stored. Domestic law enforcement authorities are not given a *carte blanche* and routine access, systematic searches or 'fishing expeditions' are forbidden.[49] Designated authorities may consult a specific system in relation to a particular case when there are *at least* reasonable grounds to consider that consultation may significantly assist in preventing, detecting or investigating a serious criminal offence. As such, consultation of data may take place not only after the commission of an offence so as to locate the perpetrator, but also preemptively. In order to verify that the conditions of access are indeed fulfilled, each EU instrument foresees the intervention of another national authority, body or entity, entrusted with that task. In urgent cases, *ex post* verification of the conditions of access, as well as transfer of data retrieved from the system to third countries or organisation, may also be possible, however the latter modality is not foreseen in the case of Eurodac.

A key issue emerging from the table relates to the threshold for establishing necessity to accessing immigration data, which is significantly different among the underlying systems. In particular, in the case of the VIS, there must be *reasonable grounds* to consider that consultation will *substantially contribute* to the fight against terrorism or other serious crimes. Besides, no specific conditions of access by Europol are foreseen in the VIS Decision. However, in the recast Eurodac Regulation it is added that necessity means that there must be 'an overriding security concern which makes the searching of the database proportionate'. Furthermore, the EES and the ETIAS Regulations drop the requirement for 'substantial' contribution and introduce the possibility that national authorities base their request on evidence *or* reasonable grounds. In both cases, the EU legislature has also clarified that there must be a substantiated suspicion that the suspect, perpetrator or victim falls within the personal scope of the database at stake. Another key difference observed in the Eurodac and EES rules is that other sources—in particular national fingerprint databases and the automated fingerprinting identification systems of all Member States—must have been exhausted prior to searching these databases. The exhaustion of other data sources is accompanied by a caveat; when there are reasonable grounds to believe that such comparison will not lead to the

49 See below as to how this safeguard will be circumvented with interoperability.

identification of the data subject (or in cases of urgency in the case of the EES) no such search must have taken place.[50]

With regard to the expedited procedure in cases of urgency, it is notable that the VIS Decision does not define when there is an exceptional case of urgency. It is in Article 19(3) of the recast Eurodac Regulation, it was clarified that such a case is when there is need to prevent an imminent danger associated with a terrorist offence or other serious criminal offences. The EES and ETIAS legal bases further specify that the danger must involve the life of a person.[51] However, both instruments do not make reference to 'exceptional' cases of urgency, but merely to cases of urgency, thus seemingly recognising that an ex-post verification of the conditions of the conditions of access may—though urgent—not qualify as an exceptional state.

4 Law Enforcement Access to Immigration Control Databases: a Privacy and Data Protection Appraisal

Both European Courts have repeatedly held that the collection and storage of personal data in centralised databases, such as the ones discussed in this article, constitutes an interference with the right to respect for private life, as enshrined in Article 7 of the EU Charter and 8 of the ECHR.[52] Similarly, the operation of databases entails the processing of personal data and as such constitutes an interference with the right to the protection of personal data. Consultation of immigration data by national law enforcement bodies and Europol amounts to a separate interference with the rights to private life and protection of personal data, in addition to the interference that initial collection and storage of personal data in databases constitutes. This approach is in line with the CJEU's judgment in *Digital Rights Ireland* concerning the retention of telecommunications data for law enforcement purposes, where it was held that access by the competent national authorities to the data constitutes an interference with the rights to private life and protection of personal data that is additional to the interference stemming from the initial collection by

50 Recital 32 of the recast Eurodac Regulation explains that this situation may arise when 'a case does not present any operational or investigative link to a given Member State'.

51 See Article 32(2) of the EES Regulation and Article 51(4) of the ETIAS Regulation.

52 The systematic collection and storage of personal data has been repeatedly found to constitute an interference with the right to private life, irrespective of whether the data will be further used, or the collection took place in an intrusive manner. In the jurisprudence of the ECtHR see *Amann v. Switzerland* (2000) 30 EHRR 843; *Rotaru v. Romania* (2000) 8 BHRC 43. For cases of the CJEU see Joined Cases C-293/12 and C-594/12 *Digital Rights* (n 10); *Tele2* (n 11).

the telecommunication providers.[53] The CJEU's pronouncement is consistent with the findings of the ECtHR in *Weber and Saravia v. Germany*,[54] where it was opined that the transmission of data to other authorities and the subsequent use by them that enlarges the group of individuals with knowledge of the personal data intercepted and can therefore lead to investigations being instituted against the persons concerned amounts a further separate interference with the right to private life.[55]

Both rights to respect for private life and protection of personal data are not absolute and any limitations may be justified, provided that the requirements of Article 52(1) of the EU Charter are met, or in ECHR terms, provided that the conditions of its Article 8(2) are fulfilled. These requirements entail an assessment of whether the limitation is provided for by law, respects the essence of the rights, meet the objectives of general interest to the EU and in line with the principle of proportionality, including whether the rules are necessary, effective and *stricto sensu* proportionate. The existence of a legitimate aim cannot be disputed; the fight against terrorist and serious crime, as well as ensuring public security, constitute objectives of general interest to the EU.[56] In relation to the legality requirement,[57] the ECtHR has been criticised for over-relying on that criterion at the expense of a proportionality assessment,[58] even though the parameters checked by the ECtHR have been the same as the ones used by the CJEU when conducting a proportionality assessment.[59] Furthermore, in the CJEU's jurisprudence, the threshold for considering an instrument not respecting the essence of the rights to private life and protection of personal data is difficult to reach[60] and it is difficult to argue the law enforcement access goes to the core of the essence of the rights in question. As for the proportionality assessment, it must be noted that though the CJEU has distinguished

53 *Digital Rights Ireland* (n 9), para. 35.

54 *Weber and Saravia v. Germany* (2008) 46 EHRR SE5.

55 *Ibid.*, para. 79.

56 See *Digital Rights Ireland* (n 9), para 42. However, see Section 4.2.2. for further considerations on the threshold for determining which offences constitute terrorist and serious one.

57 This condition requires the legislation to be accessible and sufficiently precise to the individual. See for example *Sunday Times v UK* (1992) 14 EHRR 229 para. 49; *Leander v. Sweden* (1987) 9 EHRR 433 paras 50–51.

58 See among others, De Hert, P. and Gutwirth, S. (2006). Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power' in: E. Claes, A. Duff and S. Gutwirth (Eds.), *Privacy and the Criminal Law.* Cambridge: Intersentia, pp. 61–104.

59 For an analysis see Vavoula, *Immigration and Privacy in the Law of the European Union* (n 2), ch. 1.

60 Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650.

between the interferences to the right to privacy and the right to personal data protection, it has produced a joint proportionality assessment concerning both rights.[61] This approach will be followed here as well. Against this background, this section is dedicated to employ findings from both European courts in the case of law enforcement access to EU information systems primarily established for immigration control.

4.1 *The Necessity of Law Enforcement Access: Third-Country Nationals as Risky Individuals?*

Assessing the necessity of law enforcement access requires an examination of the evidence and arguments provided by the Commission and Member States in the negotiation of each EU legal instrument governing a specific immigration database. In addition, the effectiveness of law enforcement access is preventing, detecting and investigating terrorist offences and other serious crimes is crucial; information demonstrating how successfully immigration data have been used in the law enforcement context may justify *ex post* the necessity of a measure, even the initial justifications may not have been convincing. Also, approaching the question of necessity from a chronological perspective is important, as arguments on the effectiveness of law enforcement access in relation to one database have been used in order to justify law enforcement access to another system.

4.1.1 The Necessity of Law Enforcement Access to VIS

In the case of the VIS, which represents the foundation stone of multi-purpose systems that grant access to the data to law enforcement bodies, the necessity for this additional objective is encapsulated in the preamble to the VIS Decision, where it is stated that:

> [i]t is essential in the fight terrorism and other serious crimes for the relevant services to have the fullest and most-up-to-date information in their respective fields in order to perform their tasks. The Member States' competent national services need information if they are to perform their tasks. The information in the VIS may be necessary for the purposes of preventing and combating terrorism and serious crimes and should therefore be available […] for consultation by the designated authorities.

61 See *Digital Rights Ireland* (n 9). paras 45–69; *Tele2* (n 10) paras 100–112; Opinion 1/15 (n 11) 138–231. For an analysis of this approach see González Fuster, G. 2015. Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection. *Birbeck Law Review* 2(2), pp. 263–278.

This justification is characterised, at best, as very weak. The fact that information 'may be necessary' in the fight against terrorist and other serious crimes does not automatically mean that it must be available to law enforcement bodies and Europol without further reasoning. Law enforcement access is not inherent in the system and constitutes a significant change, the necessity and effectiveness of which should have been properly assessed on a periodic basis. The latest statistical data reveal that between 2015–2017 only eight Member States performed almost 28,000 searches, 83% of which are attributed to three States (France, Germany and Switzerland).[62] Around 800 of these searches were conducted under the urgent procedure.[63] In its 2016 report on the evaluation of the VIS, the Commission suggests that out of 26 Member States, eight had never accessed the VIS for that purpose, with the use being increased.[64] Regrettably, neither report provides further information as to the number of 'hits' on the basis of VIS searches, possible false matches, follow-up procedures in cases of 'hits', including possible convictions, or information on refusals of access.

4.1.2 The Necessity of Opening Up Eurodac to Law Enforcement Authorities and Europol

Justifying consultation for criminal law purposes in the case of Eurodac has been even more problematic due to the inherent vulnerability of asylum seekers as a group of individuals in need of protection. Furthermore, as early as in 1993, before the establishment of Eurodac, the Legal Service of the Council explicitly stressed that Eurodac should not be used for other purposes, such as 'the functioning of other international instruments' or 'starting criminal investigations against asylum seekers'.[65] Testament to the complexity of the matter is the fact that the Commission presented no less than four legislative proposals,[66] including one blocked by the European Parliament,[67] before the latter would eventually cave in the desires of the Member States.[68] Strikingly

62 eu-LISA, VIS Technical Report 2018, p. 26.

63 *Ibid.*, p. 26 and p. 29.

64 COM(2016) 655 final.

65 Brouwer (n 7), p. 119.

66 COM(2008) 825 final; COM(2009) 342 final and COM(2009) 344 final; COM(2010) 555 final; COM(2012) 254 final.

67 The one of 2009.

68 For details, see Vavoula, N. (2015). The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?, in: C. Bauloz and others (Eds.), *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System.* Leiden: Brill Nijhoff, pp. 247–273.

the references to the necessity of granting access to law enforcement agencies are minimal. Recital 8 of the recast Regulation merely states that

> [i]t is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in Eurodac is necessary for the purposes of the prevention, detection or investigation of terrorist offences [...] or other serious criminal offences.

In comparison to VIS, the EU legislature is more assertive, but a connection between asylum seekers and criminality such as that inevitably made by the Regulation implies that asylum seekers as a group of people are targeted for compelling reasons. Such justification is however missing;[69] the only information available comes from three Member States, namely Austria, the Netherlands and Germany, which were the principal proponents of law enforcement access to Eurodac data.[70] However, their submission does not include any information on the criminal proceedings themselves or final convictions, while the feedback from Germany and Austria does not concern terrorism and serious crimes only, but all types of offences.

A possible explanation for insisting on law enforcement access to Eurodac is the following; it appears that at least six Member States and two other States keep asylum seekers' fingerprints in their AFIS.[71] This 'merging' design of national databases has meant that when a Member State wishes to consult information available in other Member States under the Prüm Decision,[72] if the latter State has opted for a unified database, which contains information on both criminals and asylum seekers, then the requesting state automatically has access to data on asylum seekers. However, the requested Member State

69 EDPS, 'Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of "EURODAC" for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (Recast version)' [2013] OJ C28/3 (executive summary), p. 13.

70 Council, Document 16990/12 (03.12.2012). The Dutch pointed out that between 2007 and 2011 access to national asylum seekers' fingerprints database was admitted in 356 cases and in 134 cases (38%) such comparison led to one or more criminal identifications. In Germany, where the national AFIS include the fingerprints of both asylum seekers cases and criminal cases, around 40% of criminal identifications resulted from a comparison with the fingerprints data of asylum seekers. Moreover, in Austria, which applies the same system as Germany, between 2007–2011 criminal identifications were possible in 310 cases.

71 See SEC(2009) 936 final.

72 Council Decision 2008/615/JHA [2008] OJ L210/1.

does not have that option. It thus appears that the way domestic AFIS are constructed in some Member States, and the consequent lack of reciprocity, had a significant impact in the adoption of the measure. As a result, the example of the recast Eurodac Regulation demonstrates how certain Member States exported their internal problem of how their national AFIS were designed to the EU.[73]

As for statistical data, significant discrepancies in domestic practices are evident here as well. In 2018, law enforcement authorities performed 296 searches, out of which a match was found in 201 cases.[74] These searches have taken place by nine Member States, with two thirds of them credited to Germany. Again, no information is provided as to the aftermath of the relevant match and there is no further break down as to whether the match involves a victim or a suspected perpetrator of an offence.

4.1.3 Necessity of Adding Law Enforcement to the Purposes of EES

In the case of the EES, the first Commission proposal of 2013 postponed a decision on whether to include law enforcement access to the system at a later stage, '[g]iven the high number of personal data contained in the EES'.[75] Member States were clearly dissatisfied with this approach, with no less than 20 of them expressing their wish to grant law enforcement authorities access to the EES data from the outset of its operations.[76] A concerned Commission noted the lack of proportionality between on the one hand, the data collected and stored in the EES and on the other hand, the usefulness of EES data in combating serious crime due to difficulties in ascertaining the rate of success on the basis of using such data.[77] Be that as it may, under the pressure of realising a 'Security Union'[78] in the aftermath of a series of terrorist events across Europe, the revised proposal of 2016, justified the usefulness of EES data by vague references to VIS cases, highlighting that

> Member States have reported cases of people who died violently and whose identification was only possible through accessing the VIS. Other cases reported are related to human being trafficking, terrorism or drug trafficking for which the access to VIS data allowed the investigators to make substantial progress.[79]

73 See Geddes, A. (2001). International Migration and State Sovereignty in an Integrating Europe. *International Migration* 39(6), pp. 21–42.
74 eu-LISA, Eurodac—2018 Statistics, p. 8.
75 COM(2016) 194 final, recital 23.
76 Council, Document 9863/13 (28.05.2013), p. 5.
77 *Ibid.*
78 COM(2016) 230 final.
79 COM(2016) 194 final, p. 6.

4.1.4 The Necessity of Law Enforcement Access to ETIAS Data

As for the ETIAS, the Commission proposal simply took it for granted that the ETIAS data may be useful in order to establish evidence and information related to a person suspected of having committed a crime or be the a victim of a crime.[80] The fact that the forthcoming EES, the revised proposal of which was already on the negotiating table, would also store records on visa-free travellers that will be accessed by law enforcement authorities and Europol was not commented upon.[81]

4.1.5 The Normalisation of Law Enforcement Access to Immigration Databases and the Risky Foreigner

The evolution of the legal framework on databases for third-country nationals testifies that the nexus between migration and security has solidified in an ongoing '(in)security continuum' that supplies the field of migration with security concerns related to crime control.[82] This approach whereby progressively law enforcement access found less resistance is not surprising; once resistance in relation to heated dossiers—such as Eurodac and the EES—was curved, the trend of law enforcement access was generalised and normalised. Overall, opening up databases established primarily for administrative purposes to law enforcement has become a banality, even though the analysis above demonstrates that the justification has been fragile and not convincing and the actual effectiveness of such access is still in embryonic stage with limited anecdotal information. In fact, the less information is available on the effectiveness of law enforcement access (e.g. number of perpetrators captured and crucially number of convictions), the more its necessity can be questioned. Besides, prevention of terrorist offences and serious crimes is difficult to measure, which means that the justification of the pre-emptive use of databases in the law enforcement context will probably remain elusive. Behind the trend of granting access to immigration data by law enforcement authorities are two perceptions; first, that third-country nationals collectively are *de facto*

80 COM(2016) 731 final, p. 11.

81 EDPS, Opinion 3/2017, p. 14.

82 Bigo, D. (1996). *Polices en Réseax. L' Éxperience Européenne.* Paris: Presses de Sciences Po; Bigo, D. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives* 27, pp. 63–92. This link was expressed in the Hague Programme (n 30) in para. 1.7.2: 'the management of migration flows, including the fight against illegal immigration should be strengthened by establishing *a continuum of security measures* that effectively links visa application procedures and entry and exit procedures at external border crossings. Such measures are also of importance for the prevention and control of crime, in particular terrorism'.

risky individuals suspected of criminality, the movement of whom constitutes an inherently dangerous activity that must be controlled and monitored.[83] Databases as risk technology tools are thus redeployed from the immigration control domain to the domain of the fight against impunity in an attempt to 'to feign control over the uncontrollable'.[84] In that regard, the stigmatising effect of law enforcement access, which has been stressed in *S and Marper v UK*,[85] particularly since the data are stored for a significant period of time,[86] has been largely disregarded.[87] Second, it is evident that once data has been collected and is already stored, there is no deal-breaking reason why these should not be available even for objectives unrelated to their original context. This is all the more the case considering the billions of euros invested in the development of new databases and that the individuals who are impacted by law enforcement access are foreigners, who have less leverage over state power. The result is the development of multi-purpose databases from the outset of their operations, with various objectives—including law enforcement—, which is difficult to reconcile with the data protection of purpose limitation principle. This principle suggests that data must be collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes.[88] Law enforcement access challenges the outer boundaries of the purpose limitation principle, with the threshold for incompatibility being difficult—if not impossible—to reach. This function creep, that is the widening of the purposes for which the data is used, is inherent in the functioning of immigration databases, whereby the data are casually repurposed for additional purposes other than those for which they were initially collected, without explicit justification or transparent debate. The trend is manifested either through the conceptualisation of multi-purpose databases or the gradual opening up of their purpose.[89] Furthermore, law enforcement access

83 Gammeltoft-Hansen, T. (2006). *Filtering Out the Risk Migrant: Migration Control, Risk Theory and the EU*. 52/2006, AMID Working Paper Series, Aalborg Universitet: Akademiet for Migrationsstudier i Danmark.

84 Beck, U. (2002). The Terrorist Threat: World Risk Society Revisited. *Theory, Culture & Society* 19(4), pp. 39–55, p. 41.

85 *S and Marper v UK* (2009) 48 EHRR 50, para. 122.

86 Depending on the respective legal bases, data may be held between five to ten years.

87 As regards Eurodac see for example UNHCR (2012). *An Efficient and Protective Eurodac*, Geneva: UNHCR, pp. 10–11.

88 This is particularly visible in the case of Eurodac, which was opened up to national law enforcement authorities and Europol at a later stage.

89 EDPS, 'Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of "EURODAC" for the comparison of fingerprints for the effective application of

is a prime example of preventive justice through risk assessment, whereby emphasis is placed on identifying unknown threats by assigning risk to different suspect populations.[90] The data may be used to detect not only perpetrators, but also or suspected individuals, both before and after the commission of a serious criminal offence or a terrorist attack.

4.2 *The Stricto Sensu Proportionality of Law Enforcement Access: Substantial Refinement of the Modalities of Access or Cosmetic Changes?*

Having questioned the necessity of law enforcement access despite the solidification of the trend to grant law enforcement authorities with access to immigration data, another central question emerges; are the modalities of access, as laid down in the table of Section 3, sufficiently limited in order to comply with the principle of proportionality? This corresponds to the 'strict necessity' test applicable by the CJEU[91] and the requirement in Article 8(2) of the ECHR that the interference with the right to private life is 'in accordance with law' and/or 'necessary in a democratic society'.[92] In particular, the need for clearly circumscribed conditions of access to data collected for other purposes than those for which they were originally intended to was highlighted in *Digital Rights Ireland,* where the Grand Chamber was dissatisfied with the absence of any objective criterion determining the limits of the access and their subsequent use, as well as the lack of substantive and procedural conditions concerning this access.[93] These proclamations were reiterated in *Tele2* concerning the retention of telecommunication data through national schemes.[94] Opinion 1/15 is also relevant in that respect, as the CJEU applied a strict proportionality test in the case of transfer of PNR data—that is data related to flight bookings—to the Canadian law enforcement authorities.[95]

Regulation (EU) No [.../...] (Recast version)' [2013] OJ C28/3; 'Opinion of the European Data Protection Supervisor on the proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)' (18.07.2013) pt 68; 'Opinion 06/2016 on the Second EU Smart Borders Package' (21.09.2016) pt 76. For an analysis see Benedita Menezes Queiroz (2018) *Illegally Staying in the EU—An Analysis of Illegality in EU Migration Law*. Oxford and Portland: Hart, Chapter 4 III.

90 Amoore, A. and de Goede, M. (2008). (Eds.) *Risk and the War on Terror*, Abingdon-on-Thames: Routledge.

91 According to which derogations and limitation to the protection of personal data must apply in so far as they are strictly necessary. See *Digital Rights Ireland* (n 9) para. 52.

92 For the ECtHR's approach see above Section 4.

93 *Digital Rights Ireland* (n 9), para 61.

94 *Tele2* (n 10), para 117.

95 Opinion 1/15 (n 11).

As the table above has shown, in the case of immigration databases access is governed by harmonised rules, whereby, numerous provisions are replicated with certain variations in the legal instruments. The variations in the rules denote significant efforts to refine the respective rules. No eagle's eye is required to notice that the provisions in the recast Eurodac Regulation are beefed up and are clearer than those prescribed in the VIS Decision (for instance, in relation to Europol's access to the data, the exclusion of intelligence services from designated authorities, the prohibition of transfer of data to third countries, the addition of conditions of access related to prior search in other databases), some of which are mirrored in the EES and ETIAS legal regimes. This shift is attributed to two main reasons; the controversy surrounding the reform of Eurodac, leading to extensive negotiations[96] and the timing of the EES and ETIAS proposals in the aftermath of the landmark judgments in *Digital Rights Ireland*, *Tele2* and Opinion 1/15 that imposed significant limitations to States' powers to conduct surveillance activities.[97] Be that as it may, the modalities of access raise proportionality concerns, with the problematic features involving the conditions of access, the categories of the offences for which consultation is allowed and the designated national authorities. The next sections will focus on these issues.

4.2.1 The Conditions of Access under the Microscope

Despite the obvious reforms over time, as described above, the modalities of access are disproportionate to the interferences with the rights to privacy and data protection.

First, with regards to the VIS and Eurodac, the threshold for allowing access could have been set higher by requiring the existence of factual indications as a basis for reasonable grounds.[98] Although when the VIS was negotiated, it was then submitted that this condition could *de facto* make it impossible to access the VIS for the prevention of criminal offences,[99] the substitution of 'factual indications' with 'clear indications'[100] would have been a more balanced approach. Such approach has been endorsed by the ECtHR in *Zakharov v Russia*,[101] where it was held that in order for authority to authorise surveillance, there must be reasonable suspicion against the person concerned, understood as 'factual indications for suspecting that person of planning,

96 See above, Section 2.3.
97 See Council, Document 9009/14 (05.05.2014), p. 8.
98 Mitsilegas, 'The Border Paradox' (n 8), p. 58.
99 Council Document, 5456/1/07 REV 1 (20.02.2007).
100 Council, Document 11062/06 (29.06.2006), p. 4.
101 *Zakharov v Russia* (n 12).

committing or having committed criminal acts or other acts that may give rise to secret surveillance measures …'.[102] As for the cases of the EES and ETIAS, it is notable that though a requirement of 'evidence' as a basis for the request was added, this is merely a cosmetic change because the request may still be based on reasonable grounds only.

The low threshold for law enforcement access is also evidenced when applying by analogy the CJEU's Opinion 1/15 regarding the compliance with the right to private life of the draft EU-Canada Agreement on the transfer and processing of PNR data. That case also involved mobility data being gathered for commercial purposes and transferred to law enforcement authorities. The Grand Chamber distinguished between retention and use of PNR data before the arrival of air passengers, during their stay in Canada and after their departure. Whereas the retention of data prior to their departure for Canada was found proportionate in relation to all air passengers,[103] the Court opined that the use of PNR data during the stay of passengers who have been admitted entry must be based on new circumstances justifying that use.[104] As for the retention after the departure of passengers from Canada, the CJEU took the view that passengers subjected to entry and exit checks should be regarded as 'not presenting, in principle, a risk' for terrorism and serious crime,[105] therefore, once they have left there would not appear to be a connection—even a merely indirect connection—between their PNR data and the objective pursued by the envisaged agreement which would justify that data being retained.[106] As such, the continued storage of all air passengers data after departure was deemed disproportionate and only in specific cases, where '*objective evidence* is identified from which it may be inferred that certain air passengers may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure from Canada, it seems permissible to store their PNR data beyond their stay in Canada'.[107]

Consequently, once a person has undergone screening process and particularly after leaving the national territory, the existence of a risk is minimised to the extent that storage of their personal data is no longer proportionate, unless in exceptional circumstances supported by objective evidence. These pronouncements sit at odds with the function of databases as multi-purpose tools, where the retention period of personal data is determined on the basis

102 *Ibid.*, para. 260.
103 *Ibid.*, para. 197.
104 *Ibid.*, para. 200.
105 *Ibid.*, para. 204.
106 *Ibid.*, para. 205.
107 *Ibid.*, para. 207. Emphasis added.

of their immigration control functions, but law enforcement access may still take place even if the individual, be it a short-term tourist or an irregular migrant, has long left the EU territory. A way forward would be to 'block' from law enforcement access the records of *bona fide* persons who have undergone prevetting and have been found not to pose a security risk, and/or 'mark' certain data of risky individuals on the basis of objective evidence, so that only these may be accessible by law enforcement bodies.[108]

Furthermore, that the refinement of the modalities of law enforcement access by national authorities is rendered void is evident in that the condition of prior checks in other information systems is accompanied by an 'escape clause' and that qualifying a case as urgent does not make it an exception. Therefore, whereas, the legal instruments provide some clarifications to make the modalities of access less vague, in practice the conditions of access are not substantially altered, because the revised rules are fraught with exceptions.

Moreover, access to VIS and ETIAS data could have been made dependent on exhaustion of other sources, particularly information stored in other databases, such as the national AFIS and the national AFIS of other Member States pursuant to the Prüm scheme. This would have mitigated—at least to some extent—concerns that travellers (visa and non-visa holders alike) are under suspicion of wrongdoing simply because they come from outside the EU.

In addition, access to data by Europol raises concerns for several reasons: with respect to the VIS, the differentiated regime in comparison to national authorities is unjustified and, therefore, disproportionate. The mere reference to Europol's tasks means that consultation of VIS data is not restricted to specific cases[109] and is there is no need to substantially contribute to the purpose of the access.[110] It could merely involve 'enhancing the general information position of Europol or improving the quality of Europol data'.[111] This wide access by Europol defies the exceptional character of law enforcement access and may even lead to extensive risk assessments of visa

108 The mere fact that an individual is an irregular migrant should not be considered as objective evidence basing suspicion.

109 The need to avoid routine access by Europol was highlighted by the Parliament. See Parliament, Report of 21 May 2007 of the European Parliament on the proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of the Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminals offences (COM(2004)600 final-2005/0323(CNS)), pp. 7–8.

110 Boehm, F. (2012). *Information Sharing and Data Protection in the Area of Freedom, Security and Justice—Towards Harmonised Data Protection Principles for Information Exchange at EU-level*. New York: Springer, p. 352.

111 Council, Document 5049/07 (04.01.2007), p. 4.

applicants particularly in the context of analyses of general or strategic nature. Furthermore, it must be stressed that since the retention periods may be further extended the only restriction provided in the legal bases is the existence of ongoing investigations,[112] access to immigration data may amount to an almost indefinite storage period.

Finally, in no EU instrument there is specific remark or differentiated treatment and additional safeguards foreseen in relation to minors whose personal data are accessed for law enforcement purposes. This is a crucial gap in the legislation, considering that the VIS and Eurodac will register individuals over the age of six, whereas the ETIAS does not encompass an age threshold for pre-border control application.

There is also a paradox to note; a visa holder who in the next years will provide their personal data in both the EES and the VIS may find that their personal data are accessed differently in the law enforcement context depending on whether these are stored in the EES and the VIS. Given that the EES will contain both data on visa free nationals and visa holders alike, the modalities of law enforcement access to the EES and VIS (and consequently ETIAS) should be aligned, even though visa nationals purportedly originate from countries that are risker in terms of irregular migration and criminality. Finally, this article does not purport that all categories of third-country nationals' data should be treated in the same way—for example, asylum seekers are more vulnerable that non-visa applicants and they deserve a particularly high level protection. However, where possible, the conditions of law enforcement access should be amended towards the highest common denominator, so as to reflect the ancillary and exceptional character of the access, which was highlighted by the CJEU in the case of the VIS, which in light of the above emerges as the most problematic (and therefore disproportionate) conditions of access. Furthermore, the changes to the process of law enforcement access that will take place due to the forthcoming interoperability (see below) reinforce the argument to increase the threshold.

There is also a positive reform to highlight. With the exception of the VIS, consultation of databases is not reserved only to cases where the perpetrator of a terrorist act or another serious criminal offence is a third-country national, but consultation in a specific case may involve the identification of the victim. This is certainly a welcomed addition that seems to acknowledge that third-country nationals often lack identity documents and there may not be a national database where their personal data is stored. In those cases, consultation of the relevant systems may be the last resort, particularly in cases involving migrants and asylum seekers who died at sea. It is also a means of not only

112 Boehm (n 109), p. 365.

alleviating the burden of constant suspicion that third-country nationals carry, but also avoiding the social stigma attached to their status as foreigners.

4.2.2 Defining Terrorism and Serious Crimes

The material scope of law enforcement access to immigration data involves the prevention, detection or investigation of terrorist offences and other serious crimes only.[113] This is in line with *Digital Rights Ireland* where the CJEU stressed the need for an explicit rule asserting that access and use of telecommunications data must involve merely the prevention, detection or prosecution of serious offences, given that the fight against international terrorism and serious crime as well as ensuring public security constitute objectives of general interest to the EU.[114] Furthermore, the Court highlighted in *Tele2* that in cases where the interference with the rights to private life and personal data protection is particularly serious, only the objective of fighting serious crime is capable of justifying such a measure.[115] This approach is consistent with the exceptional character of the interference, as it concerns access to immigration data that were not originally collected for law enforcement purposes. Therefore, exploring whether the definitions of terrorism and serious crime are specific and clear enables to assess whether law enforcement access is foreseen in cases which justify the interference with the rights to private life and protection of personal data.

Terrorist crimes correspond, or are equivalent to those referred to in Arts 3 to 12 of Directive (EU) 2017/541 on combatting terrorism.[116] Serious crimes are specified in Article 2(2) of Framework Decision 2002/584/JHA on the European Arrest Warrant.[117] In the case of the VIS, there is no further specification, however in the legal bases of Eurodac, EES and ETIAS, these serious crimes must be punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.[118] The fact that the offences in question are specified by reference to other EU instruments does not present a legality issue. In *Kennedy v UK*,[119] where the applicant claimed that the term 'serious crime' as set out in the British act in question was not sufficiently clear. In this regard, the ECtHR opined that as long as the term is further clarified in the interpretative provisions of the contested act and the act itself,

113 It is noteworthy that consultation of databases does not concern the prosecution of such offences, as is the case of PNR data. Compare with Directive (EU) 2016/681 [2016] OJ L119/132.

114 *Digital Rights Ireland* (n 9), para. 60.

115 *Tele2* (n 10), para. 102.

116 Directive (EU) 2017/541 [2017] OJ L88/ 6.

117 Framework Decision 2002/584/JHA [2002] OJ L190/ 1.

118 Recast Eurodac Regulation, art. 2(1)(k).

119 *Kennedy v UK* (2011) 52 EHRR 4.

the foreseeability requirement would be met.[120] In Opinion 1/15, the Grand Chamber was satisfied that the definitions of 'terrorist offences' and 'serious transnational crime' were provided with clarity and precision by requiring that they must be punishable by a maximum deprivation of liberty of at least four years or a more serious penalty and though defined by Canadian law.[121] In that respect, it must be stressed that the delineation of terrorist acts has been susceptible to consecutive reforms as a response to the phenomenon of 'foreign terrorist fighters' and new trends in terrorism. However, the inclusion of additional offences, such terrorist travel, has been rightly criticised as raising legality concerns, due to its vagueness and leading to legal uncertainty.[122] Therefore, immigration data may be consulted in relation to criminal offences that do not stand the legality test due to lack of clarity in their definition. Furthermore, with regards to the demarcation of serious crimes, it is noteworthy that the VIS Decision does not specify a particular penalty framework of the crimes encompassed, an issue that has been subsequently addressed in the cases of Eurodac, EES and ETIAS. Therefore, in the case of the VIS the lack of threshold as regards the penalty framework raises proportionality concerns. As for the rest of the databases, the barrier is rather low as well; despite the fact that in comparison to VIS, a further specification for serious crimes is provided, the barrier is also relatively low particularly in those Member States whose criminal law allows potentially long custodial sentences for fairly minor crimes.[123] Finally, the Framework Decision refers to categories of offences rather than specific crimes.

4.2.3 The Authorities Designated at the National Level: a Convoluted Legal Landscape

With the exception of Eurodac—where there is a distinction between the verifying authority and the Central Access Point—, two authorities intervene in the law enforcement access procedure; the 'designated' authority submits

120 *Ibid.*, para. 159.

121 Opinion 1/15 (n 11), paras 176–77.

122 See Standing Committee of Experts on International Immigration Refugee and Criminal Law (Meijers Committee), 'Note on a Proposal for a Directive on combating terrorism' (CM1603, 2016). With regard to the criminalisation of foreign terrorist fighters, see Vavoula, N. (2018). Prevention, Surveillance, and the Transformation of Citizenship in the 'Security Union': The Case of Foreign Terrorist Fighters, in: *Alternative, Informal, and Transitional Types of Criminal Justice and the Legitimacy of New Sanction Models in the Global Risk Society*. U. Sieber and others (Eds.) pp. 307–334, Max Planck Institute for Foreign and International Criminal Law in collaboration with Duncker & Humblot, Berlin, Germany.

123 Peers, S. and others (2015). *EU Immigration and Asylum Law.* 2nd edn, Leiden: Brill, p. 437.

the request to the Central Access Point, which acts as the verifying authority. Both authorities are decided at the national level and the list is then communicated to eu-LISA and the Commission, without control or check at EU level.[124] Member States may proceed to changes in their respective lists, which follow the same procedure of communication and publication. Furthermore, at national level, each Member State must keep a list of the operating units within the designated authorities that are authorised to access the systems. As regards the exact nature of the 'designated' bodies entrusted with the task of consulting the respective systems, the definition merely refers to authorities that are 'responsible for the prevention, detection or investigation of terrorist offences and other serious crimes', without further specification or limitation.[125] In relation to the verifying authorities, the legal bases for Eurodac, EES and ETIAS clarify that the designated and verifying authority can be within the same organisation,[126] with the preceding VIS Decision being silent on this issue. Emphasis is placed on the need for independence of the authority, which should not receive instructions from the designated authorities regarding the outcome of the verification process.[127] Similar rules exist in relation to Europol, whereby access is reserved for a specialised unit within the organisation but acting independently.

The aforementioned rules allow Member States a large amount of discretion to designate any authority they consider related to law enforcement, without further scrutiny at EU level. However, the uncritical acceptance of the lists provided by Member States has led to a series of irregularities and bad practices. A regular shortcoming of the communicated authorities is the vagueness as to the specific bodies or units within the authorities that are authorised, since in many cases a general reference to a Ministry is preferred. It may be the case that national police departments are not even explicitly listed and the relevant Ministry to which they organically belong is mentioned, whereas in other cases Member States have submitted very detailed encompassing elaborate listing of *regional* bodies and units across the Member State.[128] From

124 For the VIS list see Declaration [2013] OJ C236/1; the Eurodac list is not publicly available and has been provided by Prof. Guild who obtained it through a freedom of information request to the Commission. Ex post checks may only take place in the framework of the Schengen Evaluation Mechanism, but no infringement proceedings have been initiated against a Member State.

125 The recast Eurodac Regulation exempts intelligence services. See below.

126 Recast Eurodac Regulation, art. 6(1); EES Regulation, art. 29(3)(2); ETIAS Regulation, art. 50(2).

127 *Ibid.*

128 This is the case of the Italian and French list of authorities that may access Eurodac and the German designated authorities in the case of the VIS. Furthermore, in the Belgian, Finnish, Lithuanian, Luxembourgish and Danish list of authorities, the designated and

a technical standpoint, Member States are not required to draft the lists in a specific, detailed manner and flexibility is foreseen so as to reflect the existing divergences in administrative governance. However, from a legality point of view, this is not a satisfactory approach that allows for transparency and clarity; given that the authority must be responsible for the prevention, detection and investigation of a terrorism offence or another serious crime, the list should make clear which particular Directory or Unit within an authority is specifically designated, preferably followed by a brief explanation of the reason behind the designation. Furthermore, it is not uncommon that authorities that seem unrelated to law enforcement are also listed,[129] including military services.[130]

The flexibility allowed to Member States in allocating 'designated authorities' is further reflected in the inclusion of intelligence services. Intelligence services are traditionally understood as bodies that provide independent analysis of information related to external and internal security of state and the protection of vital national interests. Article 4(2) TEU provides that 'national security remains the sole responsibility', whereas the Law Enforcement Directive is not applicable to activities of agencies and units concerning national security.[131] However, the scope of the national security exemption particularly as regards the extent to which intelligence services are included within the term of 'competent authorities' is debatable, due to the various and often unclear separation between the areas of law enforcement and national security in individual Member States. This is particularly apparent in the case of counter-terrorism, since terrorism is regarded as a threat to both national security and to law and order. As a result, the division of competences amongst intelligence and law enforcement authorities varies throughout the EU Member States, as so do the modalities of their information exchanges. It may be the case that certain agencies at the national level are vested with tasks related to both law enforcement and intelligence analysis. That intelligence

verifying authorities enlisted are the same without further information. In addition, in Bulgaria's list of designated authorities on top of authorities such as the national police, the list refers to 'other authorities competent for the prevention, detection and investigation of terrorist acts and serious crimes' without any further specification.

129 With respect to Eurodac, Italy has designated three authorities (Command for Health Protection, Command for Agricultural and Food Policies and Command for the Protection of Labour) which do not fit. Furthermore, the VIS is accessed by the Dutch Food and Consumer Product Safety Authority and the Inspectorate of Human Environment and Transport.

130 More worryingly, military services have also been designated by Latvia (Military and Intelligence Security Service) and Poland (Military Counter-Intelligence Service and Military Intelligence Service).

131 Directive (EU) 2016/680 [2016] OJ L119/89, recital 14 and art. 2(3)(a).

services are not *a priori* completely excluded from the scope of the term is evident from the explicit exclusion of intelligence services in Article 5(1) of the recast Eurodac Regulation. Thus, unless otherwise indicated, the definition of designated authorities seems to cover intelligence services, particularly in cases whereby the boundaries of competence and their nature is mixed.[132] This limitation in the case of Eurodac, which was added during negotiations,[133] denotes that the vulnerable status of asylum seekers was taken into account in developing the modalities of law enforcement access. Be that as it may, pursuant to Article 4(2) TEU, the EU does not have competence to legislate on issues of national security, therefore it is unclear how this provision will be enforced.[134] For example, Bulgaria has included its State Agency for National Security, which is an intelligence service, among its designated authorities despite the proscription. Overall, the lack of EU competence could be interpreted as meaning that EU databases should not be accessed by intelligence services altogether, or that if such access takes place under national rules, then additional safeguards should be foreseen, such as stricter conditions of access. This approach could potentially affect the counter-terrorism activities of domestic intelligence services as they would not benefit from the data present in EU databases. However, the extent of the impact to the operation of intelligence services is directly linked to the effectiveness and usefulness of the data present in databases for the counter-terrorism functions of national intelligence agencies.

In the light of the above, a way forward would be to understand the concept of 'authorities responsible for the prevention, detection and investigation of terrorism offences and serious crimes' as an autonomous concept of EU law, guidance on the content and limits of which would be provided by the CJEU should this issue arise. A control mechanism at EU level before designation should also exist in order to prevent and combat abuses of the discretionary power enjoyed by Member States.

As for the verification that the conditions of access have been fulfilled, in *Digital Rights Ireland* and *Tele2*, the CJEU set the threshold particularly high, by requiring that prior to access by the competent national agencies, the conditions of access must be reviewed '*by a court of by an independent administrative body*'.[135] In the case of databases, it is clear that the verifying authority may be a law enforcement authority, which may also form

132 Intelligence services are listed in the VIS list by Germany, Greece, Malta, Poland and Romania.

133 Compare with the Commission proposal, COM(2012) 254 final, art. 5(1).

134 Jones, C. (2014). Analysis—11 Years of Eurodac, *Statewatch*, http://www.statewatch.org/analyses/no-235-eurodac.pdf accessed 27 August 2019.

135 *Digital Rights Ireland* (n 9,) para. 62; *Tele2* (n 10), para. 120. Emphasis added.

part of the same organisation as the agency seeking access. Though this policy choice may make practical sense, as the verifying authority could perhaps better understand the needs of a criminal investigation, it is likely that the decision regarding the fulfillment of conditions is biased, particularly if the officials involved are situated within the same organisation and/or the same premises.[136] The multiple references to the independence of the verifying authority in reaching their decisions—albeit necessary—may prove inadequate.[137] This is because once the verifying authority has concluded that the conditions of access have been fulfilled, there is no other control mechanism prior to the transmission to ensure that this assessment was indeed accurate. The sole possibility of controlling the process is *ex post* through supervision by national Data Protection Authorities, which may take place months or years later. Having access to the logs is a significant safeguard that enables accountability, however, this may not be effective for a series of reasons: if supervision takes place after months or years a number of logs may have to be checked and the national Data Protection Authority may not have the sufficient resources. Furthermore, the more the access requests, the more difficult the task for the authority will be. As a result, the strict wording of the provisions may prove ineffective in practice, and immigration data processed for law enforcement purposes more systematically than intended. Regrettably, it is difficult to so assess, as there is no information as to how many requests have been rejected by the verifying authorities.

Some good practices exist as well. In Bulgaria, Estonia and the Netherlands the task of verifying the Eurodac conditions of access is entrusted to the Prosecutor's Office. In line with the CJEU's judgment in *OG and PI*, the intervention by a prosecutorial authority, whilst institutionally independent from the judiciary, may offer significant guarantees of impartial assessment of each individual case, as long as its legal position in the Member State in question affords them a guarantee of independence from the executive.[138] Finally, another interesting example is provided by Malta, where the verifying authority for Eurodac is the Data Protection Office within the Police. This may be a satisfactory compromise solution, whereby although access is authorised by a unit within the national police, the officers are especially trained for this task.

136 Vavoula, *The Recast Eurodac Regulation* (n 67).

137 The operation of the verifying authority in Austria for Eurodac is entrusted to the Unit dedicated for Dactyloscopy (within the police, but a dedicated unit is entrusted with the task). A similar approach is taken by Belgium where the verifying authority for Eurodac is the service of judicial identification (within the police).

138 Joined Cases C-509/18 *PF*, C-508/18 *OG* and C-82/19 PPU *PI*, ECLI:EU:C:2019:457, paras 51–52.

These good practices could be applied not only in the case of Eurodac, but also to other databases. This is because, as mentioned earlier, with the progressive convergence of EU databases through interoperability, there is no real reason why the modalities for law enforcement access should not be aligned towards the highest common denominator.

4.2.4 Data Quality as a Damocles Sword

The quality of personal data stored has been a longstanding problem of the existing databases; spelling errors, lack of documentation, insufficient language skills, technical deficiencies, incorrect transcription of names into the Latin alphabet, recording of birth dates when the precise date is unknown, lack of training are only some of the reasons why databases lack data quality.[139] For example, in the case of the VIS, it has been reported that the mechanisms securing that only data of sufficient quality were entered into the system were temporarily abolished so as to speed up the registration process.[140] Even if this was a temporary solution, given that the records are retained for five to ten years (in cases of successful visa applications),[141] the effects of maintaining low quality data remain long after the rectification of the procedures. If the stored information is not of sufficient quality, the possibilities of false matches multiply, particularly when using fingerprints as search keys. A possible false match would have serious repercussions for a person wrongfully identified, namely their involvement in criminal investigations or even criminal proceedings. Finally, searches in Eurodac, EES and ETIAS based on latent fingerprints—that is incomplete fingerprints found in a crime scene—may lead to a high number of possible matches, given the wider range of possible correlations with partial or fragmentary prints.[142] As a result, the rates of error (false matches) could increase also for that reason.[143]

5 The Plot Twist: Interoperability

The analysis above merely represents one part of the story. So far, the evolution of databases has followed a gradual, *compartmentalised*, salami approach,

139 Vavoula, *Immigration and Privacy in the Law of the European Union* (n 2), ch. 3. See Fundamental Rights Agency, Opinion 1/2018, p. 30.

140 eu-LISA, 'VIS Report pursuant to Article 50(3) of Regulation (EC) No 767/2008—VIS Report pursuant to Article 17(3) of Council Decision 2008/633/JHA' (2016), p. 10.

141 VIS Regulation, art. 23.

142 EDPS, *Opinion on the Proposal of 2012* (n 89), para. 61.

143 *Ibid.*; UNHCR, *An Efficient and Protective Eurodac* (n 86), pp. 5–6.

whereby the data pots remain air-gapped, separate from each other, without the possibility to establish direct communication among them. This was originally praised as a means of safeguarding the rights to privacy and personal data protection,[144] however it is now viewed as a flaw that must be remedied. To that end, a framework for interoperability among EU databases has been created by Regulations 2019/817[145] and 2019/818,[146] with the overarching aims of improving security in the EU, allowing for more efficient identity checks, improving detection of multiple identities and assisting in the fight against irregular migration.[147] To those ends, interoperability brings together the existing and forthcoming databases for third-country nationals, by creating four interoperability components; the European Search Portal (ESP) that will enable simultaneous queries to the underlying systems, a Biometric Matching Service (BMS) that will store templates of all biometric data recorded, a Multiple Identity Detector (MID), to detect multiple identities, and a Common Identity Repository (CIR).

The CIR, in particular, will store an individual file for each person registered in the systems, containing both biometric and biographical data, as well as a reference indicating the system from which the data were retrieved. The CIR's main objectives are to facilitate identity checks of third-country nationals, assist in the detection of individuals with multiple identities and streamline law enforcement access to the underlying systems. Simplifying the procedure has been prompted by complaints at the national level that the current 'cascade mechanism' is a cumbersome procedure from an administrative perspective that results in delays and missed opportunities to uncover necessary information.[148] Regrettably, this claim is not substantiated by cases at the national level whereby such access was denied in the verification process, or was not provided on time. The fact that a procedure is cumbersome does not mean that it must be overturned altogether. Besides, in all cases, there is a mechanism of *ex-post* verification of the conditions of access in urgent cases.[149] The anecdotal and fragmented data presented above further question the claim about necessity of revising the procedure, which may simply derive from overzealous law enforcement authorities in specific Member States and are responsible for

144 COM(2010) 385 final, p. 3.
145 Regulation (EU) 2019/817 [2019] OJ L135/27 (collectively Interoperability Regulations).
146 Regulation (EU) 2019/818 [2019] OJ L135/85 (collectively Interoperability Regulations).
147 Interoperability Regulation, art. 2.
148 See the Commission proposals on interoperability, COM(2017) 793 final and COM(2017) 794 final, p. 23 and p. 45.
149 See art. 4(2) of the VIS Decision, art. 19(3) of the recast Eurodac Regulation, art. 31(2) of the EES Regulation and art. 51(4) of the ETIAS Regulation.

thousands of searches.[150] Lack of awareness of the procedure does not dictate a revision of the existing rules. Besides, if national authorities do not make use of this functionality, it is doubtful how they could ask for their reform?[151]

Under the revised rules, a two-step process is foreseen, whereby law enforcement authorities will be able to first consult all databases to check whether records on an individual exist in any of these without obtaining prior authorisation or need to fulfill specific conditions. In the event of a 'hit,' the second step is to obtain access to each individual system that contains the matching data must through the procedure prescribed for each database (hit-flag procedure).[152] Undoubtedly, interoperability will progressively lead to routine access. As noted by the EDPS, the existence of a 'hit'—that the indicated database holds a file on the individual in question—is significant, since it reveals elements of an individual's personal life, for instance that they are visa free travellers or asylum seekers, and, therefore, this first step of checking whether there is personal data in any of the underlying systems should also take place after fulfilling the specific conditions of access prescribed in the legal basis of each database.[153] Conversely, if there is no 'hit', the authorities may have still acquired some information as regards the individual in question, for example that most probably they belong to a specific group of third-country nationals. Importantly, it is hard to believe that upon finding that a database holds information on a person, the verifying authority ensuring the conditions for access have been met will not allow such access. This will be particularly the case when this function will be used in cases of *unknown* perpetrators or victims of offences, where the existence of information on the individual in a system will pre-empt the verification of the conditions of access. In other words, not only the independence and objectivity, but also the very existence of the verification process may be biased by the two-step approach. Arguably, this new function may enable national authorities to engage in fishing expeditions. Therefore, more prosecutions and/or convictions of third-country nationals may take place, merely because a pool of information exists, since no

150 The evaluation of the VIS speculates that the relative novelty of the system, lack of awareness among potential users and technical and administrative difficulties account for these discrepancies. See COM(2016) 655 final, p. 12.

151 There is no information as to whether more Member States attempt to have access but are denied so by the verifying authority.

152 Interoperability Regulations, art. 22.

153 EDPS, *Opinion 4/2018*, p. 17. See also Quintel, T. (2018). *Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention*. University of Luxembourg Working Paper 2/2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3132506 accessed 27 August 2019.

equivalent EU-wide catalogue of records on EU citizens exists. This may further sustain a divide between the EU citizens and the foreigner and raise serious non-discrimination concerns as regards the differentiated treatment between third-country nationals and EU nationals. Therefore, the establishment of the CIR may even grow the appetite to expand surveillance of movement to EU nationals with a view to even out the negative implications for third-country nationals.

6 Conclusion

This article examined the EU legal framework on the consultation of immigration databases by law enforcement authorities and Europol. By scrutinising the relevant rules, a clear trend towards the maximised exploitation of databases has emerged, which has led to the growing blurring of the boundaries between immigration control and law enforcement. Databases established primarily for immigration control purposes contain personal data on persons engaging in legitimate activities, such as applying for international protection or merely traveling for tourism or business purposes to the EU. Third-country nationals are nevertheless perceived as constituting suspect population and security risks, an understanding that they are unable to part from even if they may have undergone extensive screening processes prior to the entry (as in the case of short-stay travellers), although technological means have enabled their pre-vetting and clearance in the first place. This article has further highlighted that granting access for law enforcement purposes has become the norm, without questioning its actual necessity and effectiveness. Any initial resistance was curved in *lieu* of an extreme securitised approach, whereby the modalities of law enforcement access, whilst improved over time, still fall short of the proclamations made by the European Courts in similar cases. The case of Eurodac further reveals that the relevance of domestic policies is important in EU decision-making by enabling Member States to export national practices and problems at EU level. The analysis highlighted a series of privacy and data protection concerns, particularly with regards to the conditions of access, its material scope and the national authorities involved in the process. These concerns are fairly similar to all immigration databases, irrespective of the group of third-country nationals targeted by each database. Though it is evident that the inherent vulnerability of asylum seekers as a particular group of third-country nationals has been taken into account when drafting the conditions of access, specific policy choices remain the same. By simplifying the rules on law enforcement access, interoperability among the different systems

poses further challenges for privacy and data protection, as essentially an already disproportionate procedure will be entirely bypassed. There is indeed little room for optimism, considering that in October 2019, the CJEU released its judgment in the case of *A, B and P* concerning among other issues the use of Turkish nationals' records stored in a Dutch database for law enforcement purposes.[154] Regrettably, the Luxembourg Court did not address a relevant question by the referring court, as the applicants were not suspected of a criminal offence and their data had not been used in the framework of criminal investigations.[155] Under this approach, it is safe to conclude that the threshold for the Court to engage with questions about the proportionality of law enforcement access to personal data collected for immigration-related purposes is particularly high, thus shrinking the chances for a case actually reaching the Court. This approach disregards that law enforcement access may take place throughout the duration of the stay of an individual and long after that, thus going against its pronouncements in Opinion 1/15. It remains to be seen what the future will be bring for immigration databases and their development.

Acknowledgement

The author is indebted to Elspeth Guild and Didier Bigo for their valuable input particularly in the development of Section 4.3.3. and to the anonymous reviewer for the comments provided. Any errors remain, of course, my own.

154 Case C-70/18 *Staatssecretaris van Justitie en Veiligheid v A and Others* ECLI:EU:C:2019:823, paras 71–76.

155 For an assessment see, N. Vavoula, 'Is Processing Biometric Data of Turkish Nationals in a National Database Lawful under the EEC-Turkey Agreement? Reflections on the Judgment in A, B and P (C-70/18)' (*EU Immigration and Asylum Law and Policy*, 16 December 2019) http://eumigrationlawblog.eu/is-processing-biometric-data-of-turkish-nationals-in-a-national-database-lawful-under-the-eec-turkey-agreement-reflections-on-the-judgment-in-a-b-and-p-c-70-18/ accessed 17 February 2020.