Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?

Niovi VAVOULA*

This article examines key privacy and data protection concerns raised by the Regulations that establish a framework for interoperability between EU-wide centralized information systems processing personal data of third-country nationals (Schengen Information System II, Visa Information System, Eurodac, Entry/Exit System, European Travel Information and Authorization System, European Criminal Records Information System for third-country nationals). After a concise outline of the complex landscape within which these databases have been set up, emphasis is placed on the novelties and challenges that interoperability brings forward. In that regard, the articles evaluates the setting up of new databases, particularly the Biometric Matching Service and the Common Identity Repository – viewed through the Panopticon lens – the maximization of uses for which personal data may be destined, the revised rules on consultation of databases for law enforcement purposes, the challenge of ensuring data quality and the exercise of individual rights.

Keywords: Interoperability, Privacy, Data Protection, Databases, SIS II, VIS, Eurodac, EES, ETIAS, ECRIS-TCN

If the EU uses its law enforcement and border control tools to the full, exploits the potential of interoperability between information sources to identify any security concerns from a common pool of information, and uses the stage of entry into the EU as a key point for security checks to take place, the result will negate the ability of terrorist networks to exploit gaps. This is at the heart of the Security Union.[1]

1 INTRODUCTION

In May 2019, Regulations 2019/817[2] and 2019/818[3] were officially adopted, establishing a framework for interoperability among EU-wide information systems for

* Lecturer in Migration and Security (School of Law, Queen Mary, University of London). I am indebted to the organizers and participants of the two workshops that took place at EUI in preparation of this special issue for their comments on earlier drafts of this article. Any errors remain, of course, my own. Email: n.vavoula@qmul.ac.uk.

1 COM(2016) 602 final, 4.

2 Regulation (EU) 2019/817 [2019] OJ L135/27 (collectively Interoperability Regulations).

3 Regulation (EU) 2019/818 [2019] OJ L135/85 (collectively Interoperability Regulations).

Vavoula, Niovi. 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?'. *European Public Law* 26, no. 1 (2020): 131–156.

third-country nationals. Harvesting the possibilities offered by technological evolution and under the pressure of achieving a 'Security Union', the Regulations overall aim at improving security in the EU, allowing for more efficient identity checks, improving detection of multiple identities and assisting in the fight against irregular migration.[4] To those ends, interoperability brings together the existing and forthcoming information systems for third-country nationals (Schengen Information System II – SIS II, Visa Information System – VIS, European Dactyloscopy (Eurodac), Entry/Exit System – EES, European Travel Information and Authorization System – ETIAS, European Criminal Records Information System for third-country nationals – ECRIS-TCN),[5] by creating four interoperability components; the European Search Portal (ESP), a Biometric Matching Service (BMS), a Common Identity Repository (CIR) and a Multiple Identity Detector (MID).

This article critically evaluates the Interoperability Regulations from the perspective of fundamental rights, in particular the rights to private life and protection of personal data, as enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights respectively. To that end, the next section maps the complex landscape by tracing three historical periods in the development of European centralized databases for third-country nationals and offers a typology of key common characteristics underpinning their operation so as to inform the subsequent analysis. Then, focus is placed on the story behind interoperability and an assessment of its main components. Five themes are explored in that respect: the establishment of new databases, viewed through the lens of the Panopticon metaphor, the meta-use of stored data for additional purposes, the revised procedure for consultation of data for law enforcement purposes, the quality of personal data processed and the exercise of individual rights. It is argued that interoperability will not solve existing flaws in the legal bases and operation of the underlying systems and that rather the aggregation of data raises further privacy challenges and may accentuate existing pathologies of the underlying systems. Finally, insights into the future of interoperability are provided followed by concluding remarks.

2 THE COMPLEX LANDSCAPE OF EU CENTRALIZED DATABASES FOR THIRD-COUNTRY NATIONALS

2.1 A SKETCH

The development of European information systems may be systematically categorized in three distinct eras; the initial steps to employ technological means for the purposes of immigration control and law enforcement; the systematization of databases and the

[4] Article 2.

[5] For a detailed analysis *see* Niovi Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Databases* (Brill Nijhoff, forthcoming 2020).

gradual expansion of their capacities; and the current stage of generalized and normalized surveillance.[6] In particular, in the early 90s, the abolition of internal border controls and the evolution of technology signalled a new phase of modernization in immigration control and law enforcement. The first centralized databases were conceived; the SIS[7] and Eurodac.[8] The former, aiming at maintaining a high level of security within the Schengen area, is an intelligence tool serving both immigration and criminal law purposes through the registration of alerts on wanted or unwelcomed individuals and objects.[9] Eurodac initially supplemented the Dublin system in determining the Member State responsible for the examination of an asylum application.[10] To that end, Eurodac enabled the cross-checking of asylum seekers' and irregular border crossers' fingerprints, so as to ascertain whether a person has previously applied for international protection elsewhere.

In the aftermath of 9/11, where migration and security were heavily intertwined,[11] a new, multi-purpose database, the VIS, was conceived, with the overarching aim to modernize the administration of short-stay visas and seven ancillary objectives, including the enhancement of internal security.[12] Meanwhile, the SIS and Eurodac were armoured with new objectives and functionalities; the latter was opened up to law enforcement authorities and Europol under specific conditions,[13] whereas the former (now SIS II) was expanded to record biometric data and interlink alerts registered under different legal bases.[14]

Since the past few years, the development of centralized databases has boomed. The stake of implementing a 'Security Union' in the post-2015 era, coupled with the so-called 'refugee crisis' have resulted in increased calls to fill in perceived 'information

---

6 For an overview *see* Niovi Vavoula, *Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement?*, in *EU Law in Populist Times: Crises and Prospects* (Francesca Bignami ed., CUP, forthcoming 2019).

7 Articles 92–119 of the Convention Implementing the Schengen Agreement (CISA).

8 Regulation 2725/2000 [2000] OJ L316/1.

9 In specific, the SIS contains alerts on persons wanted for arrest; missing; sought to assist with a judicial procedure; to be served with a criminal judgment or other documents in connection with criminal proceedings; subject to discreet checks or specific checks. The system also stores data on objects (vehicles, boats, aircrafts and containers) for the purposes of discreet or specific checks, and for the purposes of seizure or use as evidence in criminal proceedings. As regards third-country nationals it records alerts on irregular migrants and third-country nationals who are convicted or suspected of committing a criminal offence carrying a custodial sentence of more than one year.

10 Regulation 604/2013 [2013] OJ L180/31.

11 Annaliese Baldaccini, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, 10(1) EJML 31 (2008); Valsamis Mitsilegas, *Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State*, 19(1) IJGLS 3 (2012).

12 Regulation (EC) 767/2008 [2008] OJ L218/60, as amended by Regulation (EC) 810/2009 [2009] OJ L243/1 (VIS Regulation); Decision 2008/633/JHA [2008] OJ L218/129 (VIS Decision).

13 Regulation 603/2013 [2013] OJ L180/1 (recast Eurodac Regulation).

14 Regulation1987/2006 [2006] OJ L381/4; Regulation 1986/2006 [2006] OJ L381/1; Council Decision 2007/533/JHA [2007] OJ L205/63.

gaps' and the emergence of centralized databases as a distinct policy field, whereby each underlying system is progressively disentangled from its border control, asylum or law enforcement roots. In this framework, surveillance of third-country nationals through the processing of their personal data is normalized[15] by doubling the number of databases. The EES[16] will operate as a 'Schengen hotel' by registering the entry and exit of all third-country nationals admitted for short-stay. The European Travel Information and Authorization System (ETIAS) will require all visa-free travellers to the Schengen area to undergo a pre-screening process to obtain authorization prior to their departure.[17] The ECRIS-TCN will enable the exchange of criminal records on their convictions.[18] In addition, the VIS and Eurodac are amidst refurbishment through an expansion of their scope both *ratione personae*[19] and *ratione materiae*, particularly by enlarging the categories of personal data collected[20] and modifying the periods for which the data are retained.[21]

2.2 A TYPOLOGY

The analysis above provides the basis for enhancing the understanding not only of the different rationale behind the establishment of each information system, but also of their common underpinnings. As it has been evident, centralized databases primarily process personal data of *different categories of third-country nationals*, be it asylum seekers, refugees, irregular migrants, short-stay tourists subject to visa requirements or visa-free travellers and convicted criminals. EU citizens are not entirely let off the hook, but their personal data are only processed in an incremental manner, for example, by the law enforcement branch of the SIS II; by the

---

15 Valsamis Mitsilegas & Niovi Vavoula, *The Normalisation of Surveillance in an Era of Global Mobility*, in *Handbook of Migration and Security* 231–251 (Philippe Bourbeau ed., Edward Elgar 2017).

16 Regulation (EU) 2017/2226 [2017] OJ L327/20 (EES Regulation).

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

18 Regulation (EU) 2019/816 [2019] OJ L135/1 (ECRIS-TCN Regulation).

19 The revised VIS will expand to include records on long-stay visa applicants, residence permit and residence card holders. *See* COM(2018) 302 final (recast VIS Proposal). The Eurodac will store personal data on irregular stayers. *See* COM(2016) 272 final (recast Eurodac Proposal). The SIS II will include alerts on all return decisions and entry bans. *See* Regulation (EU) 2018/1861 [2018] OJ L312/14 and Regulation (EU) 2018/1860 [2018] OJ L312/1. For law enforcement purposes, there is also Regulation (EU) 2018/1862 (SIS II Regulations).

20 The fingerprint process is revised. Both the VIS and the Eurodac will store the fingerprints of third-country nationals over the age of six, whereas under the current rules the fingerprints are collected from individuals over the age of 12 (VIS) and 14 (Eurodac). Furthermore, as regards Eurodac, more categories of alphanumeric personal data will be collected. *See* Arts 10–12 of the recast Eurodac Proposal.

21 According to Art. 17 of the recast Eurodac Proposal, the database will store the records on persons found irregularly crossing the external border of the EU for five years as opposed to eighteen months. The SIS II increased the retention period of alerts from three to five years.

VIS, as regards sponsors or family members of visa applicants, or in the forthcoming ECRIS-TCN in relation to dual nationals. There can be some overlapping as to the categories of individuals affected,[22] but the full picture of surveillance is only revealed if all systems are viewed collectively. Under the pressure to cover 'blind spots', in the near future, there will be no third-country national whose personal data will not be monitored through at least one database.[23]

In relation to each third-country national every database stores and enables the further processing of *a wide range of personal data* in various *fora* and contexts; before their entry, at the borders, on national territory and after they leave. The types of personal data collected may range from relatively standard (such as biographical data or travel documentation) to more intrusive (such as occupation and level of education). Importantly, with the exception of the ETIAS, databases process different types of biometrics, particularly photographs and fingerprints, which constitute special categories of personal data.[24] The preference on identifying individuals using their biological characteristics is attributed to a number of qualities that they carry, such as their universality, distinctiveness and permanence.[25]

Furthermore, databases are *adaptable, flexible and dynamic* in nature. This is particularly exemplified by their progressive beefing with additional functionalities and new purposes, as a response to perceived threats to the Union, primarily linked to terrorism, and the evolving digital technologies. As a result, the systems are used for a multiplicity of – often diverging – purposes spanning from modernizing immigration control to law enforcement, thus heavily blurring the boundaries between immigration and criminal law.[26] Indeed, every system is at the disposal of national law enforcement authorities, at least to a certain extent, either because of its law enforcement (security) mandate, as in the cases of the SIS II and the ECRIS-TCN, or because criminal law is listed as an ancillary objective, as is the cases of Eurodac, VIS, EES and ETIAS.[27]

---

22 For example, both Eurodac and the SIS II store records on irregular migrants. The EES will monitor the movement of third-country nationals covered by the VIS and the ETIAS. Convicted individuals' data will be stored in both the SIS II and the ECRIS-TCN.

23 Databases could thus be conceived as the pieces of a puzzle. For further analysis *see* Vavoula, *supra* n. 6.

24 Article 9 of Regulation (EU) 2016/679 [2016] OJ L119/1 (General Data Protection Regulation); Art. 10 of Directive (EU) 2016/680 [2016] OJ L119/89.

25 Anil Jain, Ruud Bolle & Sharath Pankanti, *Personal Identification in Networked Society* (Kluwer 1999). For an analysis on implementing biometrics at the borders *see* Commission, *Biometrics at the frontiers: Assessing the Impact on Society* (2005).

26 Valsamis Mitsilegas, *The Border Paradox: The Surveillance of Movement in a Union Without Internal Frontiers*, in *A Right to Inclusion and Exclusion? Normative Fault Lines of the EU's Area of Freedom, Security and Justice* (Hans Lindahl ed., Hart 2009).

27 For an analysis *see* Niovi Vavoula, *The Use of European Centralised Databases for Third-Country Nationals as Law Enforcement Weapons in the Fight against Impunity*, in *The Fight Against Impunity in EU Law* (Luisa Marin & Stefano Montaldo eds, Hart, forthcoming 2020).

Finally, the evolution of databases has followed a gradual, *compartmentalized* approach, whereby each system has been established under different institutional, legal and policy contexts. To date the data pots remain air-gapped, separate from each other, without the possibility to establish direct communication among them. Not for long though: the Interoperability Regulations will soon alter this structure by allowing the underlying systems to interconnect in a variety of ways. It is time to unravel that part of the databases' story.

3 COMPARTMENTALIZATION IS DEAD! LONG LIVE INTEROPERABILITY

3.1 A TALE OF TWO REGULATIONS

Debates on the possibility of interconnecting different databases first started in the aftermath of 9/11,[28] with a key issue being whether the then negotiated VIS could be linked or incorporated into the SIS.[29] The Hague Programme also mentioned interoperability both in the context of strengthening security (calling for interoperability of *national* databases or direct online access including for Europol to existing central EU databases),[30] and in the context of migration management – where the European Council called on the Council to examine 'how to maximize the effectiveness and interoperability of EU information systems'.[31] After the Madrid bombings, the European Council, in its Declaration on combating terrorism, invited the Commission to submit proposals for enhanced interoperability between SIS II, VIS and Eurodac. In its Communication on improved effectiveness, enhanced interoperability and synergies among EU databases, the Commission defined interoperability as the 'ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge'.[32] However, details on the legal aspect for the interoperability of databases were spared, as the concept was reduced to a technical rather than a legal or political matter.[33]

For years, interoperability was discussed, albeit in a sporadic manner, without being accompanied by concrete proposals.[34] Since 2015, the connection of the 'data

---

28 Council, Document 13176/01 (24 Oct. 2001).
29 COM(2001) 720 final, at 8.
30 The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, OJ C53/1, para. 2.1.
31 *Ibid.*, para. 1.7.2.
32 COM(2005) 597 final, at 3.
33 For a critique *see* Paul De Hert & Serge Gutwirth, *Interoperability of Police Databases within the EU: An Accountable Political Choice?*, 20(1–2) IRLCT 21, 22 (2006); EDPS, 'Comments on the Communication of the Commission on interoperability of European databases' (10 Mar. 2006).
34 See for instance *The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens* [2010] OJ C115/1, para. 4.2.2; Council, Document 6975/10 (01 Mar. 2010), pt 20.

pots' gained fresh impetus in order to address perceived migration and security threats. The European Council Conclusions of 18 December 2015 clearly referred to the need to ensure interoperability of all relevant systems to ensure security checks.[35] After the Brussels events of 24 March 2016, the Justice and Home Affairs (JHA) Ministers adopted a Joint Statement at their extraordinary meeting in which interoperability was treated as a matter of urgency.[36] In the Communication on stronger and smarter borders, the Commission criticized the 'fragmentation' in the current architecture of databases which are 'rarely inter-connected', thus 'there is inconsistency between databases and diverging access to data for relevant authorities', which 'can lead to blind spots notably for law enforcement authorities'.[37] As a result, four different models of interoperability were identified, which correspond to a gradation of convergence among the systems:

(1) A single search interface to query several information systems simultaneously and to produce combined results on one single screen,
(2) Interconnectivity of information systems where data registered in one system will automatically be consulted by another system,
(3) Establishment of a shared BMS in support of various information systems and
(4) Common repository of data for different information systems (core module).[38]

With a view to addressing the legal, technical and operational aspects of the different options, including the necessity, technical feasibility and proportionality of available options and their data protection implications, an Expert Group on Information Systems and Interoperability was set up.[39] In the meantime, Member States agreed in the Roadmap to enhance information exchange and information management.[40] The undertone for future development was evident and further convergence between criminal law and immigration control systems was in the making. Although the Roadmap referred to all information systems in the Area of Freedom, Security and Justice (AFSJ), related to both immigration and law enforcement, it is explicitly stated that the interlinkages between all different information exchange schemes are highlighted, which 'will contribute to ensuring the cooperation between the authorities and agencies […] and the interoperability between information systems'.[41]

---

35 Council, Document EUCO 28/15, at 3 (18 Dec. 2015).
36 Council, Document 7371/16 (24 Mar. 2016), pt 5.
37 COM(2016) 205 final, at 3–4.
38 *Ibid.*, at 14.
39 Commission Decision [2016] OJ C257/3.
40 Council, Document 9368/1/16, at 5 (06 June 2016). *See also* Council, Document 7711/16 (12 Apr. 2016).
41 *Ibid.*, at 4.

In the wait for the Commission proposals, interoperability was already embedded in the EES,[42] ETIAS[43] and recast Eurodac proposals.[44] In particular, the EES proposal prescribed interoperability between the EES and the VIS in the form of direct communication and consultation.[45] Furthermore, the revised Eurodac[46] and the ETIAS[47] were envisaged in a way that allows for future interoperability with the other databases without endorsing a particular model of such links with other systems. As it has been pointed out, the inclusion of provisions on interoperability prior to the official enactment of the relevant policy or even the adoption of specific proposals must be seen as a form of pre-empting and staging discussion on interoperability and an insertion through the back door without an agreement on its necessity and modalities.[48]

Be that as it may, the final report of the High Level Expert Group on interoperability that was created (HLEG) was released in May 2017, giving the green light for the setting up of a ESP, a shared BMS and a CIR.[49] The die had been cast and in December 2017, the Commission adopted two 'sister proposals' on interoperability; one building on the Schengen *acquis*, covering the EES, the VIS, the ETIAS and the immigration branch of the SIS II[50]; whereas the scope of the second proposal included Eurodac, the criminal law branch of the SIS II and the ECRIS-TCN.[51] The two proposals had many common provisions, but were kept separate due to differing legal bases for cooperation in each field. These proposals were revised in June 2018[52] and following speedy and rather limited negotiations, Regulations (EU) 2019/817 and 2019/818 were published in May 2019.[53]

3.2 Interoperability in a nutshell

Interoperability is defined as 'the ability to exchange data and to share information so that authorities and competent officials have the information they need, when

---

42 COM(2016) 194 final (EES Proposal).
43 COM(2016) 731 final (ETIAS Proposal).
44 Recast Eurodac Proposal, *supra* n. 19.
45 For a discussion on interoperability prior to the EES proposal of 2013 *see* Council, Document 13801/13 (19 Sept. 2013). *See* Art. 8 of the EES Regulation.
46 Recast Eurodac Proposal, *supra* n. 19, at 5.
47 *See* Art. 11 of the ETIAS Regulation.
48 Julien Jeandesboz, Susie Alegre & Niovi Vavoula, *European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection* (Study for the European Parliament, PE 583.148, 2017).
49 HLEG, Final report (May 2017). Option 2 regarding interconnectivity was to be considered on a case-by-case basis.
50 COM(2017) 793 final (collectively Interoperability Proposals).
51 COM(2017) 794 final (collectively Interoperability Proposals).
52 COM(2018) 478 final; COM(2018) 480 final.
53 It is worth noting that two more Commission Proposals were adopted in early 2019 so as to align the rules on interoperability between the ETIAS, the SIS II and the ECRIS-TCN. *See* COM(2019) 3 final; COM(2019) 4 final.

and where they need it'.[54] It must be understood as enabling information systems 'speaking to each other' and an evolutionary tool that enables further uses through the aggregation of data from different sources. In particular, interoperability will allow faster access to information, enable the detection of multiple identities, facilitate identity checks of third-country nationals and streamline access for law enforcement purposes. In addition to the three main components envisaged by the HELG, the ESP, the shared BMS and the CIR, interoperability further encompasses the creation of the MID.

In particular, the ESP will enable competent authorities to simultaneously query the underlying systems to which they have access and the combined results will be displayed on one single screen.[55] Even though the screen will indicate in which databases the information is held, access rights will remain unaltered and will proceed following the rules of each database.[56] Furthermore, the BMS will generate and store *templates* from all biometric data recorded in the underlying systems,[57] thus effectively becoming a new database compiling biometric templates from the SIS II, VIS, Eurodac, EES and ECRIS-TCN and will substitute separate searches. The template does not contain the full (biometric) information as contained in the collected sample, but only represents the particular features selected by the algorithm(s).[58] An extension of the BMS and a novel tool, the MID will use alphanumeric data stored in the CIR and the SIS II with the aim of detecting multiple identities. The MID will create links between identical data to indicate whether the individual is lawfully registered in more than one systems or whether identity fraud is suspected.[59] Therefore, its dual purpose is to facilitate identity checks for *bona fide* travellers and combat identity fraud.[60] Four types of links are envisaged; white (in the case of clear identity)[61]; yellow (in the case of unclear identity)[62]; green (in the cases of confused identity, such as two different persons with similar data)[63]; and red (in the case of identity fraud).[64] At the core of interoperability lies the CIR, which 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.[65] At the

[54] Interoperability Proposals, *supra* nn. 50–51, at 2.
[55] Articles 6–11.
[56] Recital 15.
[57] Articles 12–16.
[58] Els Kindt, *Privacy and Data Protection Issues of Biometric Identifiers* 98 (Springer 2013).
[59] Articles 25–36.
[60] Recital 39 and Art. 25.
[61] Article 33.
[62] Article 30.
[63] Article 31.
[64] Article 32.
[65] Articles 17–24.

heart of interoperability lies the CIR that will combine data from the VIS, Eurodac, EES, ETIAS and ECRIS-TCN, thus not the SIS II, and its main objectives will be to enable identification of TCN's without (proper) travel documents, assist in the detection of individuals with multiple identities and streamline the procedure for consulting databases for law enforcement purposes.[66] As regards the latter issue, 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 authorization or need to fulfil 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).[67]

4 INTEROPERABILITY: THE MESSY 'GLUE' THAT BINDS THEM ALL

With the operationalization of interoperability, the landscape of European information processing through centralized databases will be forever changed. Interoperability *by default* 'disrespects the importance of separated domains and cuts through their protective walls'.[68] Compartmentalization, which was once praised as a means of safeguarding the rights to privacy and personal data protection,[69] is viewed as a flaw that must be remedied.

4.1 The emergence of a digital 'pan-gnosticon': (Unlawful) mass surveillance in disguise

Perhaps the elephant in the room as regards to the operationalization of interoperability involves the masked setting up of new databases – the BMS, the CIR and the MID- based on the combination and aggregation of data from different sources (albeit the latter will not hold personal data). The fancy wording that is used ('component' and 'repository') that has been carefully selected and prevails in the discussions should not distract from the reality of creating massive catalogues of third-country nationals at EU level who are either administratively or criminally linked to the EU that will store personal data over a significant period of time.

---

66 Article 17(1).
67 Article 22.
68 De Hert & Gutwirth, *supra* n. 33, at 27.
69 COM(2010) 385 final, at 3. 'The compartmentalised structure of information management that has emerged over recent decades is more conducive to safeguarding citizens' right to privacy than any centralised alternative'.

Whereas the MID will not hold personal data, as it will merely store links among records that definitely or possibly match, a central question that arises is whether the BMS will process *personal* data, since it will merely store *templates* of the biometric identifiers included in each individual file. Thus, the safeguards deriving from data protection law, whereby the processing of personal data is a prerequisite, would not apply. From the outset, it must be stressed that legal scholarship is not conclusive as to whether biometric templates qualify as personal data. According to Article 4(1) of the GDPR, 'personal data' is defined as:

> any information relating to an identified or identifiable natural person … ; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

On the one hand, it has been argued that finding the person of the template would require unreasonable efforts.[70] On the other hand, it is undeniable that a template also contains unique information about a person and whereas the intervention of technology would be required to 'read' it and establish the link with an individual, this does not prevent the conclusion that a template constitutes personal data.[71] The Article 29 Working Party had excluded biometric templates from being considered as personal data only '[i]n cases where [these] are stored in a way that no reasonable means can be used by the controller or by any other person to identify the data subject'.[72] Even if the transformation of biometrics into templates were to be deemed as a means of pseudoanonymization, the GDPR explicitly states that such data, which could be attributed to a natural person by the use of additional information – in this case such additional information would derive from the actual samples stored in each database – should be considered as information on an identifiable natural person.[73] In the light of the above, the BMS emerges as a powerful database essentially storing biometric materials (dactylographic data and facial images). The fact that the ETIAS is not encompassed within the BMS – because it will not record biometrics – bears no significance to this finding, since biometrics of visa-free travellers are nonetheless captured by the EES upon their entry to the Schengen area.

The case of the CIR is equally problematic and constitutes an interference with the rights to private life and protection of personal data. In essence, the CIR will

---

70 Pascal Kolkman & Robert van Kralingen, *Privacy en nieuwe technologie*, in *Privacyregulering in theorie en praktijk* 410 (J. M. A. Berkvens & Corien Prins eds, Kluwer 2007).

71 Kindt, *supra* n. 58, at 94–100. *See* Mirja Gutheil et al., *Interoperability of Justice and Home Affairs Information Systems* (Study for the European Parliament, PE604.947, 2018).

72 Article 29 Working Party, Working Document on Biometrics 5 (WP80, 2003).

73 Recital 26.

contain an individual file for each person registered in at least one of the databases. Each file will compile data that are recorded in the different systems – logically separated in accordance with the system from which the data was originated – and will comprise of a series of biographical data (names, including aliases, date and place of birth, nationality, sex, travel documents). The system that holds the full record will also be indicated. The CIR, therefore, will generate general profiles of millions of third-country nationals who have crossed or even considered crossing the EU external borders (e.g. failed visa applicants). It also equates information systems such as the ECRIS-TCN with a clear law enforcement mandate with the rest, which include law enforcement as a secondary objective only. As such, the CIR will become an overarching system and a significant step towards mass and indiscriminate surveillance of practically the entire foreign population with an administrative or criminal law link to the EU.

The Foucaultian 'Panopticon' metaphor is particularly popular in discussions about mass surveillance and may be useful to comprehend the effects of interoperability.[74] In essence, the creation of massive digital catalogues will enable domestic authorities to *see* all different groups of third-country nationals. Repetitive references to *'blind spots'* that need to be covered so that everyone could be *seen* fits well with the analogy.[75] Whereas each database on its own is a means of establishing visibility over a significant period of time,[76] interoperability will enable domestic authorities to enhance such visibility and *know* all the different categories of third-country nationals better, by assembling records from the different systems and combine the different personal data to create richer profiles regarding their movement and administrative or criminal procedures that they have undergone. Moving beyond its traditional understanding, the 'pan-opticon' (coming from the ancient Greek 'πάν' (all) + 'οπτικόν' (of sight)) is progressively replaced by the 'pan-gnosticon' ('πάν' (all) + 'γνωστικόν' (of knowledge)), an emerging know-it-all surveillance system, whereby authorities will be able to achieve total awareness of the identities of the individuals, with the ultimate aim of preventing, deterring, controlling, or in more neutral words 'managing' people. By recording third-county nationals' identities, everyone will be marked and sorted out. As such, the EU shall be able to exert significant power on a large proportion of the non-EU population so that they are excluded from the territory and/or disciplined within.

---

74 Michel Foucault, *Discipline and Punish – The Birth of Prison* (Editions Gallimard 1975). In the context of databases *see* Dennis Broeders, *The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants*, 22 Int'l Soc. 71 (2007).

75 Interoperability Proposals, *supra* nn. 50–51, at 2.

76 In reality, these catalogues may even amount to permanent registrations (e.g. frequent travellers whose personal data are stored in the EES, or apply for authorization via the VIS or the ETIAS).

The conceptualization of the CIR as a tool enabling mass surveillance of millions of third-country nationals is key in assessing its proportionality. In a series of judgments, the EU Court of Justice has placed important limits to Member States' surveillance powers by scrutinizing the personal scope of the legal instruments in question and implying a distinction between of mass and targeted surveillance. In Opinion 1/15, concerning the transfer of Passenger Name Record (PNR) data from the EU to Canada for law enforcement purposes, the Grand Chamber found that such transfer and use of data prior to their entry to Canada would not amount to a system of unlawful generalized surveillance, given that the personal scope of the scheme was limited to those travelling from the EU to Canada.[77] Emphasis was placed on the purpose of the systematic retention and use of PNR data, which is to facilitate security and border control checks.[78] Conversely, in *Digital Rights Ireland*[79] and *Tele2 Sverige and Watson*[80] concerning the retention of telecommunications metadata for law enforcement purposes, the Grand Chamber was adamant in proscribing mass surveillance, where it involved 'practically the entire EU population' without exception or limitations.[81] The aforementioned pronouncements are central here. Whilst each database *on its own* may not qualify as establishing generalized and indiscriminate surveillance pursuant to Opinion 1/15, because it involves only a fraction of third-country nationals, the CIR as a new database combining materials from the underlying systems ticks, including special categories of personal data (biometrics) all the boxes to be considered as unlawful mass surveillance. The lack of connection with the SIS II does not alter the fact that all categories of non-EU nationals will be captured by the CIR, as that system includes alerts on irregular migrants and criminals, which are already captured by Eurodac and ECRIS-TCN respectively. The disproportionality is compounded by the fact that the proclaimed aims of the CIR as a means of identifying individuals is achieved by the individuals systems on their own without the need to have recourse to an overarching single information system. Finally, the CIR is at odds with proclamations of the Commission, which seems to recognize the significant implications of a system as massive and all-encompassing as the CIR. In its Communication on information management in the Area of Freedom, Security and Justice it was stressed that an overarching EU information system would 'constitute a gross and illegitimate restriction of

---

77 Opinion 1/15 (26 July 2017) ECLI:EU:C:2017:592, paras 186–189.

78 *Ibid*.

79 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Ireland* (08.04.2014) ECLI:EU:C:2014:238.

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

81 *Digital Rights Ireland, supra* n. 79, paras 56–59; *Tele2 Sverige and Watson, supra* n. 80, para. 105.

individuals' right to privacy and data protection and pose huge challenges in terms of development and operation'.[82] In that case, reference was made to a single information system on third-country nationals from scratch, but the CIR is not far from that.

A final point must be made here. The creation of the ESP as a message broker whereby national authorities shall be able to consult a single interface for fast query results is the sole component of interoperability that does not involve the setting up of a new database. Nonetheless, its necessity and proportionality may also be challenged given that their primary purpose has been to increase efficiency of searches, rather than filling in real operational gaps. Furthermore, it has been correctly pointed out that the ESP is merely set up to enable the implementation of new information systems.[83]

4.2 Of uses and meta-uses of personal data: Databases as a moving target

One of the flagship arguments in favour of interoperability of information systems has been the fact that it will not frustrate existing limits on *access* rights of national authorities.[84] In other words, no new categories of national authorities shall be able to have access to the personal data apart from those already envisaged to have access to the information stored already. The danger of altering access rights had indeed been voiced by the European Data Protection Supervisor (EDPS), who highlighted the potential over-reach of those having access to databases under interoperability noting that the latter 'should never lead to a situation where an authority, not entitled to access or use certain data, can obtain this access via another information system'.[85]

This represents only one side of the story. What is at stake is the *use* of personal data that will be attached to new purposes, which are not always found in the respective legal bases, and their *meta-use* due to their combination and aggregation. These uses should be considered as new interferences with the rights to privacy and personal data protection. A prime example in that respect involves the use of databases in the context of the MID to detect persons with multiple identities. Whereas the VIS and the EES list identity fraud among their objectives,[86] Eurodac's mandate is primarily linked to the operation of the Dublin system as a supporting mechanism

---

82 COM(2010) 385 final, at 3.

83 Article 29 Working Party, Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration, WP266 4 (2018).

84 *See* Recitals 17, Arts 6(1), 18(3).

85 European Data Protection Supervisor, Opinion on the Communication of the Commission on Interoperability of European Databases (10 Mar. 2006).

86 *See* Art. 2(c) of the VIS Regulation and Art. 6(1)(i) of the EES Regulation.

and does not specify such use of the Eurodac data. In order to match this function of Eurodac under the Interoperability Regulations, another amendment of the legal basis will be necessary. It is striking that in its report, the HLEG even suggested that the mandate of Eurodac should be further expanded to include 'security' in its purposes in order encompass.[87] Thus, interoperability seems to have become *an end in itself* that defines the purposes and sets the uses for personal data that may have been already collected and stored.

Additional concerns are raised in relation to Article 20 of the Interoperability Regulations, which empowers national *police* authorities to query the CIR with the biometric data of a person over the age of 12 taken during an identity check in presence of the person in question, for the sole purpose of identifying them.[88] The circumstances under which identity checks may be carried out are: (1) where a police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity; (2) where there are doubts about the identity data provided by a person; (3) or the authenticity of the travel document or another credible document provided by a person; (4) or the identity of the holder of a travel document or of another credible document; or (5) where a person is unable or refuses to cooperate.[89] Where a search indicates that data on that person is stored in the CIR, the querying authority may access to the record retained in the CIR and obtain a reference to the underlying data to which the record belongs.[90] A police authority will perform a query if they are so empowered through national legislative measures that must specify the precise purposes of the identification, designate the competent police authorities and prescribe the procedures, conditions and criteria of such checks.[91] The purposes for which queries may take place are those referred to in Article 2(1)(b) and (c) of the Regulations, namely the prevention and the combating of illegal immigration; the high level of security, including the maintenance of public security and public policy and safeguarding security in the territories of the Member States.

This novelty that has been rightly characterized as the 'most controversial use(s)'[92] of interoperability raises serious proportionality concerns. In essence, Article 20 merely enables random identity checks to be carried out at the national

---

87 HLEG, *supra* n. 49, at 53.

88 Article 20(1). The age limit was added at the behest of the Parliament. Identity checks for minors below the age of 12 are permitted if it is in the best interests of the child.

89 *Ibid*. Compare to the Commission Proposals where these circumstances were not listed. *See* Council, Document 14691/18, 163–170 (10 Dec. 2018).

90 Article 20(3).

91 Article 20(5).

92 Tony Bunyan, *The 'Point of No Return' Interoperability Morphs into the Creation of a Big Brother Centralised EU State Database Including All Existing and Future Justice and Home Affairs Databases*, Statewatch, http://statewatch.org/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf (accessed 10 Aug. 2019).

level on the basis of biometric data in the CIR and Member States that wish to benefit from this facility must circumscribe relevant provisions at the national level. The only requirement is that the purposes of identity checks must be aligned with those of fighting irregular migration and ensuring a high level of security. The wording of the latter purpose is identical to the overarching aim of the SIS II,[93] which as mentioned earlier, has a strong law enforcement dimension. The necessity of creating of massive database with records on all third-country nationals for facilitating identity checks is not demonstrated. The conduct of random identity checks for both immigration and law enforcement purposes has been accepted by the EU Court of Justice in several cases[94]; in *Melki*, the Court found that where national measures would not have an effect equivalent to border controls, random police checks, the aim – of which may be to 'combat cross-border crime' – are permissible.[95] Furthermore, in *Staatsanwaltschaft Offenburg*, the checks were aimed not only at preventing or terminating unlawful entry into German territory, but also at preventing criminal offences.[96] However, the EDPS is right in pointing out that these objectives are unduly vague and do not explain whether these police checks will take place under immigration control or law enforcement procedures.[97] This is crucial as regards to the application of relevant data protection safeguards, in particular as to whether the higher standards of the General Data Protection Regulation (GDPR) or the less strict ones in the Police Directive will apply.[98] The addition of specific circumstances under which police authorities are authorized for identification checks in the adopted text does not compensate for the lack of clarity. On the contrary, the lack of common criteria and purposes may lead to highly divergent rules and practices at the national level, whereby third-country nationals, or EU nationals looking like foreigners, may find themselves being subjected to different practices depending on how proactive a police authority in a Member State is. As noted by the Article 29 Working Party (now European Data Protection Board), 'querying the CIR … could result in a very large number of accesses given the volume of identity checks led by police authorities'.[99] Extensive identity checks by police authorities may fuel discriminatory practices based on increased suspicion towards specific categories of indivi-

---

93 Article 1 of the SIS II Regulations.
94 In line with Art. 21 of the Schengen Borders Code.
95 Joined cases C-188/10 and C-189/10 *Aziz Melki* (C-188/10) and *Sélim Abdeli* (C-189/10) [2010] ECLI:EU:C:2010:363, paras 69–70.
96 Case C-9/16 *A v. Staatsanwaltschaft Offenburg* (21 June 2017) ECLI:EU:C:2017:483, para. 46.
97 European Data Protection Supervisor, Opinion 4/2018, at 12–13.
98 *Ibid*.
99 Article 29 Working Party, *supra* n. 83, at 11.

duals, which may proceed to identification checks to third-country nationals on the spot solely on the basis of extensive (racial) profiling,[100] rendering their status on the territory particularly precarious and sustain a hostile environment. The checks may simply be based on appearance, irrespective of the behaviour of the individual or specific circumstances giving rise to a risk of breach of public order. The risk of discriminatory practices is recognized in the Regulations as it is stated that 'Member States shall take into account the need to avoid any discrimination against third-country nationals'.[101] Though this is a welcomed addition to the original text, the wording 'shall take into account' is not particularly strong. Importantly, no further limitations as to intensity or frequency have been elaborated.[102] This is central since the identity checks against the CIR will take place on the basis of biometrics, which are special categories of personal data, thus requiring additional, strict safeguards. Limitations concerning the coercion in submitting the fingerprints for comparison would have been significant in that respect. The absence of relevant rules on identity checks seems to repeat the story of the invalidated Data Retention Directive.[103] In *Digital Rights Ireland*[104] and *Tele2 Sverige and Watson*,[105] both on the retention of telecommunication metadata for law enforcement purposes, the EU Court of Justice stressed the need 'for sufficient safeguards, … to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data'.[106] It may be the case that the relevant procedures and criteria will be subject to future harmonization, but this may result in a race to the bottom by embracing the most State-friendly rules.

Furthermore, the cases of the MID and the CIR are key in understanding the destructing, deregulating potential of interoperability. It negates the relevance of the purpose limitation principle[107] by essentially enabling databases to be used for almost any purpose as long as this is not incompatible with the original purpose for which the data have been originally collected. The multiple reconfigurations of the systems over time denote that the threshold for such 'incompatibility' is impossible

---

[100] *See* Teresa Quintel, *Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals*, 4 EDPLR 470 (2018).

[101] Article 20(5).

[102] This has also not been done by the EU Court of Justice. *See* Case C-278/12 PPU *Atiqullah Adil* (19 July 2012) ECLI:EU:C:2012:508.

[103] Directive 2006/24/EC [2006] OJ L105/54.

[104] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Ireland* (08 Apr. 2014) ECLI:EU:C:2014:238.

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

[106] Paragraph 66. This view is shared by the Art. 29 Working Party, *supra* n. 83, at 12; EDPS, *supra* n. 97, at 13 and the Fundamental Rights Agency, Opinion 1/2018, at 26–27.

[107] *See* EDPS, *supra* n. 106, at 62; Art. 29 Working Party, *supra* n. 83, at 11.

to reach and the limits of these systems are far from being exceeded. The fact that the CIR will include both personal data collected and further processed for traditional law enforcement purposes (ECRIS-TCN) and personal data of immigration nature that will be used for the identification of individuals in multiple *fora* is probably the deathblow to the purpose limitation principle and generally to the right for respect for private life enjoyed by third-country nationals. This logic does not correspond to the traditional understanding of migration control, but rather fosters, validates and accentuates the transformation of information systems for third-country nationals to 'security systems' their reconceptualization as quasi-intelligence tools.[108]

One more consideration is due. The fact that access rights are defined in the legal bases does not mean that this arrangement is immune to flaws. It must be recalled that the designation of national competent authorities takes place at the national level,[109] on the basis of national administration particularities. Member States are merely required to communicate their list of competent authorities to the Commission, which are then published in the Official Journal and may be amended accordingly. Consequently, there is no involvement, intervention or control at EU level, as long as that access is provided to national authorities entrusted with the tasks that correspond to the purposes of each database. This unfiltered system of designation that provides extensive discretion to Member States may be prone to abuses, misunderstandings and arbitrary or unclear designations. This is more than mere hypothesis. It is beyond the scope of the present article to illustrate the numerous irregularities in the designation of national authorities granted access to databases. It suffices here to mention that despite the explicit prohibition in the Eurodac Regulation that intelligence services may not have access to the system,[110] Bulgaria has designated its State Agency for National Security. As regards Austria, instead of pinpointing specific authorities designated at the national level, it rather vaguely refers to 'border control authorities' and 'law enforcement authorities' without further specification.[111] As a result, whilst access

[108] *See also* Niovi Vavoula, *Interoperability of European Centralised Databases: Another Nail in the Coffin of Third-Country Nationals' Privacy*?, EU Immigration and Asylum Law and Policy, http://eumigrationlawblog.eu/interoperability-of-european-centralised-databases-another-nail-in-the-coffin-of-third-country-nationals-privacy/ (accessed 10 Aug. 2019).

[109] For the SIS II see, Notices from Member States [2019] OJ C222/1. For Eurodac *see* eu-LISA, List of designated authorities which have access to data recorded in the Central System of Eurodac pursuant to Art. 27(2) of the Regulation (EU) No 603/2013, for the purpose laid down in Art. 1(1) of the same Regulation (Apr. 2019). The list of authorities that are granted access to Eurodac for law enforcement purposes is not publicly accessible. For the VIS *see* Notices from Member States [2016] OJ C187/4; Notices from Member States [2013] OJ C236/1.

[110] Article 5(1) of the recast Eurodac Regulation.

[111] The findings are part of an ongoing project carried out by Didier Bigo, Elspeth Guild and Niovi Vavoula.

rights are not altered at EU level, interoperability does nothing to rectify an existing pathogenic feature and conceals the fact that whilst new categories of authorities will not be granted access, the list of authorities is nonetheless created at the domestic level and is amended at will.

4.3 Streamlining law enforcement access by circumventing an already problematic procedure

There is an additional reason why the CIR constitutes a disproportionate, thus unlawful interference with the right to privacy and personal data protection. As mentioned earlier, one of the main novelties of the interoperability architecture facilitated by the CIR involves the streamlining of the procedure for allowing national law enforcement authorities to consult the databases as one of their ancillary objectives. Under the current rules, law enforcement access to the VIS and Eurodac and the forthcoming EES and ETIAS is reserved to specific cases for the prevention, detection and investigation of terrorist offences[112] and other serious crimes.[113] Consultation of the relevant data stored in a specific database is subject to conditions custom-made for each database and *ex ante* verification that these conditions are fulfilled by a verifying authority.[114] In particular, with certain variations, access must be necessary for the prevention, detection or investigation of terrorist offences or other serious crimes, it must be necessary in a specific case, thus ruling out systematic comparisons, and there must be at least reasonable grounds to consider that the information contained in the database accessed will substantially contribute to the objective of addressing terrorism or other serious offences.[115] It is also outside the scope of this article to analyse why the rules on law enforcement access to centralized databases raise proportionality concerns.[116] In a nutshell, whereas the lack of routine access is a welcomed feature – after all these databases are not law enforcement tools – the existing safeguards are insufficient in numerous respects. First, with the exception of Eurodac, intelligence services are not excluded from the authorities that Member States may designate.[117] Furthermore, the conditions of access as such do

[112] As defined in Directive (EU) 2017/541 [2017] OJ L88/6.

[113] Serious crimes are deemed those listed in Art. 2(2) of Framework Decision 2002/584/JHA [2002] OJ L190/1.

[114] Whereas the rules are relatively similar, discrepancies remain. For example, in the cases of Eurodac, the EES and the ETIAS prior consultation of national fingerprint databases, as well as the automated fingerprinting identification systems (AFIS) of other Member States must have been conducted (albeit with exceptions).

[115] In the case of the EES and ETIAS, either 'evidence' *or* 'reasonable grounds' are required. *See* Art. 32(1)(c) of the EES Regulation and Art. 52(1)(c) of the ETIAS Regulation.

[116] For an analysis *see* Vavoula, *supra* n. 27.

[117] Compare Art. 5(1) of the recast Eurodac Regulation with Art. 3 of the VIS Decision, Art. 29 of the EES Regulation and Art. 50 of the ETIAS Regulation.

not provide for a high threshold, with the argument being forward that evidence or factual indications would be more appropriate.[118] Moreover, whereas in the cases of the Eurodac, EES and ETIAS, additional requirements have been inserted mandating the exhaustion of other sources before seeking access to them, the rules are fraught with exceptions.[119] Finally, from an operational perspective, it has been highlighted that authorities that are not supposed to have access may still be able to consult the data indirectly through colleagues who have wider access rights.[120]

Streamlining 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.[121] In other words, this procedure, whereby access is relatively circumscribed and subject to certain safeguards due to its exceptional character, should be further simplified and watered down for the sake of enhancing law enforcement capacities. Regrettably, this claim is not substantiated by cases at the national level demonstrating that 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.[122] A few contextual remarks are also due; first, with regard to the VIS, the latest statistical data reveal that between 2015 and 2017 eight Member States only performed almost 28,000 searches, 83% of which to three Member States (France, Germany and Switzerland).[123] Around 800 of these searches were conducted under the urgent procedure.[124] As for Eurodac, in 2018, law enforcement authorities performed 296 searches, out of which a match was found in 201 cases. These searches have taken place by nine Member States, with two thirds credited to Germany.[125] In both cases, no information is provided as to the aftermath of the relevant match and in the case of Eurodac there is no further breaking down as to whether the match involves a victim or a suspected perpetrator. The aforementioned data reveal significant discrepancies in domestic practices and still fragmentary and inconsistent application, questioning the claim about the necessity to revise the procedure, which may simply derive from overzealous law enforcement

[118] Council, Document 5456/1/07 (20 Feb. 2007).
[119] Compare Art. 5 of the VIS Decision, Art. 20 of the recast Eurodac Regulation, Art. 32 of the EES Regulation, Art. 52 of the ETIAS Regulation.
[120] Fundamental Rights Agency, *Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security* 25–26 (2017).
[121] Interoperability Proposals, *supra* nn. 50–51, at 23 and 45.
[122] *See* Art. 4(2) of the VIS Decision, Art. 19(3) of the recast Eurodac Regulation, 31(2) of the EES Regulation, 51(4) of the ETIAS Regulation.
[123] eu-LISA, VIS Technical Report 2018, at 26.
[124] *Ibid.*, at 26 and 29.
[125] eu-LISA, Eurodac – 2018 Statistics, at 8.

authorities that are responsible for thousands of searches.[126] 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, how could they ask for its reform?[127]

The pronouncements of the EU Court of Justice are particularly useful when scrutinizing the revised procedures for law enforcement access. In *Digital Rights Ireland* and *Tele2*, the CJEU made clear first that further transfer to data enlarging the pool of authorities having access to personal data constitutes a further interference with the rights to private and data protection[128] and second, as mentioned earlier, that such access should be subject to strict conditions and prior verification that those conditions have been met by a verifying authority, which must be either a judicial or independent, administrative one.[129] 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.[130] 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 preempt the verification of the conditions of access. In other words, not only the independence and objectivity, but also the very existence of a verifying authority 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/

---

126 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, at 12.

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

128 *Digital Rights Ireland, supra* n. 79, para. 35. *See* the judgment of the European Court of Human Rights in *Weber and Saravia v. Germany* (2008), 46 EHRR SE5.

129 *Digital Rights Ireland, supra* n. 79, para. 62; *Tele2 Sverige and Watson, supra* n. 80, para. 120.

130 European Data Protection Supervisor, Opinion 4/2018, at 17. *See also* Teresa Quintel, *Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention*, University of Luxembourg Working Paper 2/2018, SSRN Paper https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3132506 (accessed 10 Aug. 2019).

or convictions of third-country nationals may take place, merely because a pool of information exists, since no 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.

4.4 Data quality: A thorny issue

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.[131] 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.[132] As such, data quality suffered. Even if this was a temporary solution, it must be recalled that the records are retained for five to ten years (in cases of visas granted), thus the effects of maintaining low quality data remain long after the rectification of the procedures. These findings are corroborated by immigration controls officers who confirm that they have identified significant mistakes in the entry into the data systems over the course of their work.[133] If the stored information is not of sufficient quality, any aggregation of data through interoperability may have led to incorrect processing, irregularities and false matches, with significant repercussions for third-country nationals, particularly in the case of the MID for checking identity fraud.[134] Interoperability will only be as successful as the stored data is. In order to rectify this thorny issue, the Regulations empower the EU Agency that is responsible for the

[131] Vavoula, *supra* n. 5. *See* Fundamental Rights Agency, *supra* n. 106, at 30. *See* as regards the SIS II *see also* COM(2016) 880 final, at 11.

[132] 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) 10.

[133] *Inaccurate Data in Schengen System 'Threatens Rights'*, euobserver, https://euobserver.com/tickers/140468 (accessed 10 Aug. 2019).

[134] Evelien Brouwer, *Interoperability and Interstate Trust: A Perilous Combination for Fundamental Rights*, EU Immigration and Asylum Law and Policy, https://eumigrationlawblog.eu/interoperability-and-interstate-trust-a-perilous-combination-for-fundamental-rights/ (accessed 10 Aug. 2019). For the implications of false matches *see* Case C-291/12 *Schwarz v. Stadt Bochum* (17 Oct. 2013) ECLI:EU:C:2013:670.

operanational management of these information systems (e-LISA) to establish automated data quality control mechanisms and common data quality indicators, so that only data fulfilling the minimum quality standards.[135] This is certainly welcomed however, as mentioned above, it is not sufficient to ensure data quality of new data, but further to establish procedures for *ex post* correction of incomplete and/or flawed records.

4.5 Individual rights only on article?

A final point regarding the exercise of individual rights merits some attention. Individuals whose personal data are recorded in the systems are entitled to a series of rights; to receive information as regards the purposes for and authorities processing their personal data and to seek access, rectification and deletion of their information, subject to specific rules and variations depending on the mandate of each database.[136] The low turnout in the exercise of individual rights is a key recurring problem of the current information systems architecture.[137] On the one hand, the systematization of data collection leaves no other choice to individuals but to provide their personal data in order to adhere to administrative and criminal law procedures envisaged under Union law. They cannot be considered as having consented to these procedures either. On the other hand, when other fundamental rights are at stake, such as in the case of asylum seekers, perhaps interest in safeguarding their privacy and personal data protection is secondary. Thus, it will only be in situations where individuals are adversely affected that such exercise of individual rights is expected and that is if the individual in question is in a position to exercise their rights financially, legally, or even physically, which may not be the case. This perplex landscape will be further complicated by interoperability, as individuals will lose foreseeability and thus control over how their personal data will be further processed in the future, especially since their data will be used in a multiplicity of contexts and subject to consecutive change. As a result, the right to information, as a basis for the exercise of the rest of the rights accorded to individuals, may be all the more difficult to be exercised. The Interoperability Regulations seem to acknowledge this convoluted framework therefore a web portal with public information on the exercise of individual rights is foreseen.[138] The extent to which this is sufficient is debatable, as

[135] Recital 48 and Art. 37.
[136] Compare Art. 67 of Regulation 2018/1862, Arts 52–53 of Regulation 2018/1861 (both on the SIS II), Arts 37–38 of the VIS Regulation, Art. 14 of the VIS Decision, Art. 29 of the recast Eurodac Regulation, Arts 50–52 of the EES Regulation, Art. 64 of the ETIAS Regulation, Art. 25 of the ECRIS-TCN Regulation.
[137] For example, as regards the VIS *see* COM(2016) 655 final, at 12.
[138] Article 49.

the web portal must contain information on the substance of the rights, not merely on whether they exist and what procedures must be followed. Furthermore, this provision seems to be a back-up solution, in cases individuals are not properly informed about their rights at the stage of collection. As for the effectiveness of the web portal, it remains to be seen whether the exercise of individual rights will increase in the future.

5 INTEROPERABILITY: A BOTTOMLESS BARREL

The aforementioned considerations are based on interoperability as envisaged in the Regulations. However, that is not the end of the story. Defined in a flexible manner, interoperability heralds the beginning of a new era of personal data processing heavily grounded on technology-based trust among Member States and increased automation in information exchange under simplified rules that represent a race to the bottom. The Interoperability Regulations are merely the stepping stone towards an emerging architecture of total information awareness in an omniscient Union, whereby decentralized structures, not limited to surveying third-country nationals, will be interconnected for the sake of realizing a Security Union. It will not be surprising if new proposals emerge in the near future linking systems established under the Prüm framework,[139] the PNR Directive[140] or the Advance Passenger Information Directive[141] with one or more of the interoperability components. This was already mentioned by the HELG in its final report[142] and explicitly mentioned by the Commission in its Proposals.[143] Customs databases on goods will also follow with the discussions progressing even though interoperability is still in the making.[144] These efforts will confirm not only that the nature of databases is utterly changed to become 'security systems' but also the longstanding view that modern technological advents, particularly the most controversial ones, are first 'tested' on third-country nationals before they make their way to EU nationals.[145] The interoperability apparatus will thus be used to survey and manage the very own subjects the security of whom is meant to ensure. As it has eloquently been pointed out, interoperability seems indeed to be the 'point of no return'.[146]

---

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

140 Directive (EU) 2016/681 [2016] OJ L119/132. This fits within the emergence of a Travel Intelligence Architecture. *See* Statewatch, Europol foresees key role in 'the EU travel intelligence architecture', http://www.statewatch.org/news/2018/nov/eu-pnr-iwg-update.htm (accessed 10 Aug. 2019).

141 Directive 2004/82/EC [2004] OJ L 261/24.

142 HLEG, *supra* n. 49, at 38–40.

143 Interoperability Proposals, at 5.

144 Council, Document 5574/19 (29 Jan. 2019).

145 Ben Hayes, *NeoConOpticon: The EU Security-Industrial Complex* 35 (Transnational Institute/Statewatch 2009). *See* Katja Lindskov Jacobsen, *Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation*, 14(1) Citizenship Stud. 89 (2010).

146 Bunyan, *supra* n. 92; EDPS, *supra* n. 97, at 10.

6 CONCLUSION

Interoperability is much more than a buzzword and a panacea to address security and migration concerns; it is a conscious political choice that has become the 'Trojan Horse' towards the silent disappearance of the boundaries between law enforcement and immigration control and the radical intensification of surveillance of all mobile third-country nationals. The privacy and data protection implications are significant; As Bunyan has noted, it is not far-fetched to characterize interoperability as a decisive step towards a single EU information system at the service of an EU Big Brother.[147] Interoperability not only frustrates the in-built safeguards in the operation of the systems, but also changes the interpretation of key data protection principles, such as purpose limitation, which is confirmed as almost a dead letter principle. Whereas interoperability is marketed as a means of ensuring streamlined and seamless access to the stored data, this simplification further adds to the complexity from an operational and importantly from a legal standpoint and is bound to deteriorate existing operational flaws in the legal bases, whilst creating new challenges. With that step completed, it is only a matter of time before PNR, Prüm and customs data also make their way into interoperable centralized databases, so as to 'rectify' the imbalance between the treatment of third-country nationals and EU citizens in terms of surveillance. Interoperability is the latest nail on the coffin of third-country nationals' privacy; databases have progressively proliferated and their functions expanded without having been litigated in terms of fundamental rights compliance before the European Courts. In an era where strategic litigation seems to be the way forward, is it possible for centralized databases to find their way into courts, or will we have to wait until data surveillance hits our own door?

[147] Bunyan, *supra* n. 92.