Interoperability Between EU Policing and Migration Databases: Risks for Privacy

Hartmut ADEN*

The interoperability initiative passed in May 2019 as Regulations (EU) 2019/817 and 818 seeks new strategies for identifying dangerous individuals who use false or multiple identities. The EU's databases in the Area of Freedom Security and Justice (AFSJ) for policing and migration purposes will be interconnected. This constitutes a paradigm shift for purpose limitation as a core element of data protection. This article identifies regulatory patterns and shortcomings in the technical and legal data protection arrangements of the interoperability regulations. The legal framework for data protection in the EU has developed considerably with the General Data Protection Regulation (GDPR) 2016/679 and with Directive 2016/680 for policing and criminal justice. The European Data Protection Board, a multilevel accountability forum in which European and national data protection authorities cooperate has been established. From a trans-disciplinary legal, public administration, and public policy perspective, this article analyses the regulatory patterns and institutional settings established for the upcoming interoperability of databases for policing and migration.

Keywords: EU migration and policing databases, police information sharing, interoperability, data protection, privacy, accountability, eu-LISA, Europol, Schengen Information System, Visa Information System, EU external borders

1 INTRODUCTION

In May 2019 the EU Council of Justice and Home Affairs (JHA) ministers passed Regulations (EU) 2019/817 and 818,[1] aiming to deliver interoperability between EU information systems for 'security, border and migration management', based on proposals published by the European Commission in December 2017.[2]

* Professor of German and European Public Law, Public Policy and Public Administration at the Berlin School of Economics and Law/Hochschule für Wirtschaft und Recht (HWR Berlin) in the Department of Police and Security Management, Deputy Director of the Berlin Institute for Safety and Security Research (FÖPS Berlin), and Data Protection Officer of HWR Berlin. Email: Hartmut.Aden@hwr-berlin.de.

1 OJ L 135 of 22 May 2019, at 27 (Regulation 2019/817) and 85 (Regulation 2019/818).

2 The 'package' included: European Commission, *Proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226*, Brussels: COM(2017) 793 final; European Commission, *Proposal for a regulation of the European Parliament and of the Council on establishing*

Aden, Hartmut. 'Interoperability Between EU Policing and Migration Databases: Risks for Privacy'. *European Public Law* 26, no. 1 (2020): 93–108.
© 2020 Kluwer Law International BV, The Netherlands

The separation into two regulations is due to the different Treaty bases. While both regulations refer to Articles 16(2) and 74 Treaty on the Functioning of the European Union (TFEU), Regulation 2019/817 for interoperability in the field of borders and visa is based on Article 77(2) (a), (b), (d), and (e), while Regulation 2019/818 for interoperability in the field of police and judicial cooperation, asylum, and migration is based on Articles 78 (2)(e), 79(2)(c), 82(1)(d), 85(1), 87 (2)(a), and 88(2) TFEU.

The *interoperability* of IT systems and databases has been a major topic for law enforcement cooperation in Europe and beyond since the early 2000s.[3] With the institutionalization of police cooperation in the framework of the EU's 'third pillar' in the 1990s, the number of cooperation venues and IT solutions used for cooperation purposes multiplied. If information is fragmented and distributed over several cooperation venues and databases, security problems may escape the attention of the relevant security agencies. This problem was identified after the terrorist attacks of 11 September 2001 in the United States, as the US landscape of security agencies had been highly fragmented and only loosely coordinated before 2001. Therefore, the fragmentation of relevant information was increasingly perceived as a risk in Europe as well.

Cases in which terrorists and criminals managed to travel to and within the EU using false or multiple identities have been brought forward to justify the new regulatory approach for interoperability.[4] The logic behind interoperability is that security agencies should have instruments facilitating identification of individuals who are particularly dangerous in order to prevent them from committing terrorist attacks. However, it is particularly challenging to shape new instruments in a way which will not lead to a massive extension of the surveillance of many or even all EU and third country citizens travelling to and in Europe.

The legal framework for data protection in the EU has developed considerably with the General Data Protection Regulation (GDPR) 2016/679 and with Directive 2016/680 for data protection in the field of policing and criminal justice. However, this framework covers neither data processing by EU agencies, such as Europol or the *European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice* (eu-LISA), nor specific technological developments, such as big data analysis. The legal bases are highly fragmented. Each EU agency and database is governed by a separate regulation, including specific data protection rules in each case. Therefore, the institutional

---

a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), Brussels: COM(2017) 794 final.

3 B. A. Bischof & R. Schellen, *Interoperabilität im Europäisierungsprozess der Strafverfolgungsbehörden* (Kassel: Kassel University Press 2012).

4 European Commission, *supra,* n. 2.

arrangements for data protection vary considerably between the relevant EU agencies and databases. Regulations 2019/817 and 818 include specific data protection rules for the interoperability approach and therefore add to the already existing regulatory fragmentation and (over-)complexity. A trend towards a specific multilevel accountability forum in which European and national data protection authorities cooperate can be observed with the establishment of the *European Data Protection Board* by the GDPR. This may contribute to more coherence in the future.

From the perspective of data protection and privacy, interoperability constitutes a fundamental paradigm shift, compared to the IT and data protection philosophy that has been governing the databases for the European Union's *Area of Freedom, Security and Justice* (AFSJ) for many years. The *Schengen Information System* (SIS), the database *Eurodac* containing the fingerprint data of all asylum seekers, and the *Visa Information System* (VIS) on applicants for a Schengen visa and their hosts have been separate thus far, and access to them was primarily limited to those involved in the purposes for which each database had been established.[5] This was an easy and obvious strategy to implement purpose limitation as one of the main principles of the fundamental right to data protection and privacy according to Article 8 Charter of Fundamental Rights of the European Union (CFR). Interoperability fundamentally changes this approach – even more as new databases that are currently being established are included: the *Entry Exit System* (EES) registering all third country nationals entering or leaving the EU, the *European Travel Information and Authorization System* (ETIAS) for travellers from third countries who do not need a visa, and the sub-section of the *European Criminal Records Information System* documenting criminal convictions of third country nationals (ECRIS-TCN).[6] All these databases will be integrated into the interoperability framework established by Regulations 2019/817 and 818.

Against this backdrop, this article explores, from a trans-disciplinary legal, public administration, and public policy perspective, the regulatory patterns and

---

[5] For an overview over the legal instruments governing policing and migration databases: H. Aden, *Europäische Rechtsgrundlagen und Institutionen des Polizeihandelns* (*Abschnitt N*), in Handbuch des Polizeirechts, (H. Lisken (co-founder), E. Denninger, M. Bäcker & K Graulich eds, 6th ed., Munich: C.H. Beck, 2018, 1617–1705); F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice* 256 ff. (Heidelberg: Springer 2012); European Commission, *Communication from the Commission to the European Parliament and the Council on Strengthening Law Enforcement Cooperation in the EU: the European Information Exchange Model (EIXM)*,Brussels: COM (2012) 735 final (7 Dec. 2012).

[6] For an overview: R. Bossong, *Intelligente Grenzen und interoperable Datenbanken für die innere Sicherheit der EU. Umsetzungsrisiken und rechtsstaatliche Anforderungen* 10 ff. (Berlin: Stiftung Wissenschaft und Politik 2018).

institutional settings that have been developed for data protection and privacy[7] in transnational policing in the EU, shortcomings in the existing legal and institutional framework, and new problems related to the interoperability regulations.

2 INTEROPERABILITY IN THE LANDSCAPE OF POLICE INFORMATION SHARING AND DATA PROTECTION IN THE EU

Information sharing is a core element of transnational cooperation among law enforcement agencies. Since the early initiatives for international police cooperation that led to the establishment of Interpol's predecessor in the early twentieth century,[8] improving the access to information held by police agencies abroad has been the main motivation for police cooperation initiatives.[9] In the age of advanced information technology, access to databases has become an important tool for sharing information. This is mostly a 'hit/no hit' access, where a 'hit' only occurs if a name or other data entered by an officer matches data that has been previously stored in the database. In some cases, it can also be reading or writing access to the content of the database.

In the past, police information sharing in the EU multilevel system has often been criticized for a lack of coherence. The European Commission was not very successful with attempts to convince law enforcement agencies to limit the number of 'channels' used for information sharing.[10] Since the Treaty of Lisbon, the Commission has been trying to strengthen the EU's role as 'service provider' for the Member States' law enforcement agencies. This can be interpreted as part of the Commission's strategy to gain power and influence in a field that is still largely characterized by intergovernmental patterns of policy-making – even a decade after the end of the EU's pillar architecture and thus the intergovernmental third pillar for *Justice and Home Affairs*.[11] Facilitating the use of AFSJ databases and

---

7 *See* M. Tzanou, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance* 21 ff. (Oxford: Hart Publishing 2017) on the relationship between data protection and privacy.

8 *See* C. Fijnaut, *A Peaceful Revolution. The Development of Police and Judicial Cooperation in the European Union* 10–46 (Cambridge, Antwerp and Chicago: Intersentia 2019).

9 *See* M. Anderson, M. den Boer, P. Cullen, W. Gilmore, C. Raab & N. Walker, *Policing the European Union* 49 ff. (Oxford: Clarendon Press 1995); M. Deflem, *Policing World Society: Historical Foundations of International Police Cooperation* (Oxford: Oxford University Press 2002); C. Fijnaut, *Revolution or Evolution Through the Treaty of Lisbon: Police Cooperation in Europe in a Broader Historical Context*, in *Police Cooperation in the European Union Under the Treaty of Lisbon. Opportunities and Limitations* 25–48 (H. Aden ed., Baden-Baden: Nomos 2015).

10 *See* M. Busuioc & D. Curtin, *The Politics of Information in Internal Security: Information Sharing by European Agencies*, in *The Politics of Information. The Case of the European Union* 260–276 (T. Blom & S. Vanhoonacker eds, Basingstoke: Palgrave Macmillan 2014); European Commission, *supra*, n. 5.

11 *See* M. den Boer, *Police Cooperation. A Reluctant Dance with the Supranational EU Institutions*, in *Policy Change in the Area of Freedom, Security and Justice* 114–132 (F. Trauner & A. Ripoll Servent eds, Abingdon: Routledge 2015).

maximizing their usefulness for law enforcement is part of this service, objectives that also characterize the new interoperability setting.

In the EU multilevel system, two types of police information sharing can be observed: *centralized approaches*, in which databases play a major role, and *network-based approaches*. The interoperability of policing and migration databases is part of the centralized approach to police cooperation that has been streamlined since the late 2000s by the transfer of multiple institutional settings into formal EU agencies, such as *Europol*, the *European Border and Coast Guard Agency (Frontex*), and *eu-LISA*, for the management of the EU's policing and migration databases.

Initially, for the centralized AFSJ databases, even the institutional structure was far from being homogeneous. The *Schengen Agreements* and the legal basis for Europol began as international public law treaties in the 1980s and 1990s. The technical infrastructure for the *Schengen Information System* was run in Strasbourg, based on a specific arrangement among the participating Member States. *Eurodac* and the VIS started as instruments of common immigration, asylum, and visa policy that were transferred from the EU's third pillar to the European Communities' framework with the Treaty of Amsterdam. Access to these databases for law enforcement agencies remained part of the EU's third pillar.[12] Therefore, in its transitional period between the Amsterdam and Lisbon Treaties, the legal regime governing the centralized AFSJ databases became highly fragmented, with parallel instruments for the first pillar and third pillar elements. Even several years after the end of the 'pillar architecture', this fragmented legal framework has not yet been fully replaced by more coherent instruments. Some of the old intergovernmental third pillar instruments have yet to be replaced by EU regulations or directives.[13]

For the management of interoperability, eu-LISA, the *European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice*, established in 2011 and located in Tallinn (Estonia),[14] plays a crucial role. While the physical IT infrastructure remains in Strasbourg in a unit now belonging to eu-LISA, bundling the governance of major parts of the EU's IT infrastructure for the AFSJ in a single agency is not only a step towards more coherent governance of the databases but also facilitates the implementation of interoperability.

In some respects, the interoperability regulations go far beyond previous initiatives for a more coherent security governance. The reactions to terrorist

---

12 For the VIS: H. Aden, *Visainformationszugangsgesetz – VISZG*, in *Sicherheitsrecht des Bundes. Kommentar* 1079–1094 (W.-R. Schenke, K. Graulich & J. Ruthig eds, 2d ed., Munich: C.H. Beck 2019).

13 *See* Aden, *supra,* n. 5 for an overview.

14 *See* Fijnaut, *supra,* n. 8, at 364 ff. and Aden *supra*, n. 5, marginal no. n. 190 ff. on the creation and tasks of eu-LISA.

attacks in the US in 2001 and in Europe, especially those in London and Madrid in 2004 and 2005, led to intensified police cooperation.[15] The more recent terrorist attacks in Paris, Nice, Brussels, Liverpool, Berlin, and other places in Europe, combined with high numbers of refugees arriving in Europe (especially in 2015), opened a window of opportunity for additional initiatives combining security and anti-migration purposes. Political pressure to react to these incidents resulted in a majority vote in the European Parliament and the Council for European *Passenger Name Records* (PNR) and for the *Entry/Exit System* (EES) meant to establish more effective surveillance of those entering or leaving the EU. Members of Parliaments concerned with data protection and the proportionality of the restrictions to civil liberties that these initiatives involve lost influence under the impression of terrorist attacks.[16] The legal rules governing the EES, foreseeing an additional centralized database, are laid down in Regulation (EU) 2017/2226. The database will store data on the place and time when non-EU citizens enter or leave the EU. When non-EU citizens exceed the maximum duration of their stay granted to them according to the visa, the Member States will receive an automated warning message (Article 1). Interoperability between the EES and the VIS is already foreseen in the Regulation (Article 8). This means that particularly sensitive data will be shared more easily in the future. In addition, a ETIAS will be established, allowing highly standardized pre-checks of nationals from a number of third countries for which visas are not required.

The massive use of biometric data for identification purposes is a central characteristic of the EES and the interoperability regulations. Biometric data plays a central role for the technical implementation of interoperability, based on the idea that fingerprints and other biometric data enable security agencies to identify individuals with a high level of certainty. Thus, if the same biometric data is related to more than one name or passport, this is an indicator of an individual using a false or more than one identity. Therefore, a *Shared Biometric Matching Service* (BMS), a *Common Identity Repository* and a *Multiple-Identity Detector* (MID) are core instruments foreseen in the interoperability regulations. These facilities are meant to add a meta-infrastructure as a kind of roof on top of the

---

[15] R. Bossong, *The Evolution of EU Counter-Terrorism. European Security Policy After 9/10* (London: Routledge, 2013); T. Balzacq & S. Léonard, *Information-Sharing and the EU Counter-Terrorism Policy: A 'Securitisation Tool' Approach*, in *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe* 127–142 (C. Kaunert & S. Léonard eds, Basingstoke: Palgrave Macmillan 2013). C. Kaunert, *European Supranational Governance in the Area of Freedom, Security and Justice* 63ff (Manchester and New York: Manchester University Press 2010); J. D. Occhipinti, *The Politics of EU Police Cooperation. Toward a European FBI?* 147ff (Boulder, Colorado: Lynne Rienner 2003).

[16] *See* J. P. Albrecht, *EU Police Cooperation and Information Sharing: More Influence for the European Parliament?,* in *Police Cooperation in the European Union Under the Treaty of Lisbon – Opportunities and Limitations* 223–233 (H. Aden ed., Baden-Baden: Nomos 2015).

existing and future AFSJ databases that will be accessible for the relevant agencies in a *European Search Portal* (ESP).

Centralized databases and their interoperability are only one element of enhanced police cooperation as it has emerged in the EU in the past decades. Beyond this centralized support infrastructure, police agencies use formal and informal *network approaches* to exchange information. Transnational police networks are a much older phenomenon than EU police cooperation,[17] as they have existed since the early days of international police cooperation already.[18] Police agencies sometimes maintain intensified working relationships with agencies in neighbouring countries or in partner cities abroad. Police officers from different countries meet at official or informal occasions and then use their contacts to exchange information during transnational investigations. For police officers in the EU, *Justice and Home Affairs* cooperation offers numerous occasions to meet colleagues from other countries, for example at seminars organized by the *Collège Européen de Police* (CEPOL) or in *Joint Investigation Teams*.[19] *Liaison officers* that Member States send to *Europol* or exchange bilaterally are a specific form of network-based horizontal cooperation. Article 9 of Council Decision 2009/371/JHA on Europol, now replaced by Europol Regulation (EU) 2016/794, legally institutionalized the exchange of information by Europol liaison officers.

Another network-based strategy for information sharing is the establishment of police and customs cooperation centres in the border regions. Instead of exchanging information via administrative and judicial hierarchies, police and customs officers share a common office near the border where they cooperate directly on all kinds of cases with a trans-border aspect. Today, trans-border cooperation centres exist in numerous regions along the internal borders.[20]

In practice, centralized databases and network-based approaches will often be used in parallel. During a criminal investigation or after an arrest, the databases will be consulted, and the agencies' or personal networks may additionally be mobilized.

---

17 *See* Fijnaut, *supra*, n. 8 for an overview.

18 *See* Deflem, *supra*, n. 9; Fijnaut, *supra*, n. 9.

19 *See Liaison Officers: Essential Actors in Transnational Policing* (M. den Boer & L. Block eds, The Hague: Eleven International 2013).

20 Compare. A. Gruszczak, *Police and Customs Cooperation Centres and Their Role in EU Internal Security*, in *EU Borders and Shifting Internal Security* 157–175 (R. Bossong & H. Carrapico eds, Heidelberg: Springer 2017).

3 PRIVACY AND DATA PROTECTION FOR EU POLICING AND MIGRATION DATABASES: NEW CHALLENGES RELATED TO INTEROPERABILITY

Interoperability of policing and migration databases leads to new challenges from the perspective of data protection and privacy. Therefore, the data protection provisions of the interoperability regulations have been particularly contested during the law-making process. However, as the adoption of the regulations took place under time pressure before the elections for the European Parliament in May 2019, these challenges were hardly noticed by a broader public. This section analyses the data protection rules as adopted in the interoperability regulations and their shortcomings that have been partly softened by the European Parliament's intervention for improved data protection during the ordinary legislative procedure.

The interoperability regulations implement some of the basic requirements of data protection, as they are already the standard in recent regulations governing the single AFSJ databases involved. For example, the responsibility for internal and external data protection monitoring has been defined.[21] Rules for keeping logs as an essential precondition for assuring accountability towards data protection authorities have been established.[22] However, in view of the high number of individuals concerned, the sensitivity of the biometric data to be processed in the interoperability framework, and the specific challenges for purpose limitation due to the merger of data collected for very different purposes, the data protection provisions are still underdeveloped, even after the European Parliament's intervention during the law-making process.

3.1 Over-complexity and fragmentation of data processing and data protection rules

The distribution of the legal framework for the interoperability of policing and migration databases over two parallel, but very similar, regulations symbolizes the complexity that still governs the AFSJ a decade after the Treaty of Lisbon entered into force. The Treaty provisions, as the European Commission understands them in proposals for new legislation, do not allow a full merger of rules distributed over several legal acts under the former 'third pillar'.

---

[21] Arts 44, 51–53 Regulation (EU) 2019/818.

[22] *See* Arts 10, 16, 24 and 36 Regulation (EU) 2019/818; as the wording of Regulations (EU) 2019/817 and 818 is mostly very similar (if not the same), the following sections only refer to Regulation (EU) 2019/818 for police and judicial cooperation, asylum and migration; the analysis can be transferred to Regulation (EU) 2019/817.

The data protection rules for the single AFSJ instruments are highly fragmented too.[23] Each instrument is based on a specific regulation including separate data processing and data protection rules for each database. The policing parts of the *Schengen Information System*, one of the core elements of the interoperability tools, will be based on Regulation (EU) 2018/1861 in the future. This regulation refers to four other regulations as the 'applicable legislation' for data protection related to the SIS (Article 51). Only in recent years has the legal framework governing the AFSJ databases become somewhat more coherent. Where the pre-Lisbon legal bases have been replaced by new EU law instruments, the *European Data Protection Supervisor* now plays a coordinating role for data protection for Europol according to Regulation (EU) 2016/794. This is also foreseen in the interoperability regulations.[24] Nevertheless, the legal framework for data processing and data protection remains fragmented.

Europol's databases are only partly integrated into the interoperability framework. The Europol Regulation (EU) 2016/794 defines very specific data processing and data protection rules that no longer describe the IT systems to be used by Europol, as had been the case in Europol's previous legal bases. The Europol Regulation only lists the categories of data that the agency may process. On the one hand, this reflects a move from describing data processing to an increasing emphasis on the individual's right to privacy.[25] On the other hand, this makes the extent to which data processing may occur less transparent for citizens, as the way in which Europol can make use of 'weak' data, for example on suspects and witnesses, is no longer explicitly mentioned in the regulation.

The interoperability regulations add another layer of data processing and data protection rules[26] that have to be applied in combination with the rules governing the single databases and with general EU data protection law.[27] The interoperability regulations therefore include numerous cross-references to the other regulations in the area. Thus, the legal framework for data protection regarding EU migration and policing databases tends to become over-complex. The complexity of the rules makes their application more challenging for the security agencies involved and leads to a risk of incorrect application. From the perspective of the individuals concerned, who would like to understand for what purposes their personal data is being used and

---

[23] *See* the critique by Boehm, *supra*, n. 5, at 171 ff. & 398 ff.; this has not fundamentally improved in recent years.

[24] Aden, *supra*, n. 5, marginal no. n. 126 ff.; Art. 52 Regulation (EU) 2019/818.

[25] Compare P. de Hert & V. Papakonstantinou, *Data Protection. The EU Institutions' Battle Over Data Processing vs Individual Rights*, in *Policy Change in the Area of Freedom, Security and Justice* 178–196 at 184 (F. Trauner & A. Ripoll Servent eds, Abingdon: Routledge).

[26] *See* Arts 40 to 53 Regulation (EU) 2019/818.

[27] *See also* the critique by the European Data Protection Supervisor (EDPS), *Opinion 4/2018 on the Proposal for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems* 9 ff. (Brussels: EDPS 2018).

how long it will be stored, this complexity reduces the transparency that general EU data protection law requires as part of lawful and fair data processing.[28]

3.2 Fragmented responsibility in a multilevel framework

Fragmentation characterizes not only the legal bases for the AFSJ data processing but also their governance and accountability structures. While patterns such as the participation of Member States' authorities in decision-making characterize all of them, each database has its own governance structure and specific institutional settings for data protection, mostly involving representatives from the Member States' data protection authorities.

The selection of directly-applicable EU regulations for new pieces of legislation does not lead to full harmonization. Often regulations include multilevel elements that attribute tasks and responsibilities to the Member States. The interoperability regulations include some directly binding rules, while numerous other issues are left to the Member States. For example, not only the EU agencies involved are data controllers for the data to be processed in the interoperability framework, but in some respect the Member States' authorities are also involved. Thus the rules laid down in the interoperability regulations establish a system of combined horizontal and vertical multilevel fragmentation of the responsibility for data processing.[29] While the GDPR has defined the role of a data controller in order to bundle and strengthen the responsibility for the implementation of appropriate technical and organizational measures for a high level of protection and rights of natural persons,[30] the interoperability regulations opt for fragmented responsibility.

Multilevel fragmentation also characterizes the rules laid down in the interoperability regulations, attributing specific data protection tasks to Member States' administrations. For example, log files for the use of the interoperability instruments are foreseen at the EU level, to be kept by eu-LISA. As these log files at the EU level do not include information about the authorized user who initiated a query, additional log files have to be kept by the relevant administrations at the Member States' level. As log files include personal data on the officers involved, this fragmentation may be perceived as data protection-friendly. However, if access to the information available in the log files is needed, i.e. in cases of alleged misuse of the interoperability instruments, identifying the individuals responsible will make it necessary to combine

---

[28] Article 5 (1)(a) Regulation 2016/679 (GDPR) and Art. 4 (1)(a) Directive (EU) 2016/680; *see also* P. C. Johannes & R. Weinhold, *Das neue Datenschutzrecht bei Polizei und Justiz. Europäisches Datenschutzrecht und deutsche Datenschutzgesetze* 64 (Baden-Baden: Nomos 2018).

[29] Article 40 Regulation (EU) 2019/818.

[30] Article 24 Regulation (EU) 2016/679 (GDPR).

the log files at the EU and Member States' [?] level. This specific (over-) complexity leads to the risk that the identification may fail.

3.3 Conflicts between interoperability and purpose limitation

The storage of data in the interoperability tools constitutes an extension of the purposes for which the data has been originally collected.[31] Until now, separate data silos for each database have been a core element of data protection for EU policing and migration databases. This will no longer work with databases interconnected by the interoperability tools. Therefore, the interoperability framework is more than just another step towards increased Europeanization of standardized police information-sharing within centralized databases. Interconnections created between the already existing and even future AFSJ databases by the *Common Identity Repository (CIR)* and the meta-research facilities put into question the traditional paradigm of data protection as it was established for the AFSJ databases over the past decades.

According to Article 8 CFR, personal data must be processed fairly *for specified purposes*. The data processed in the *Common Identity Repository* and the *Biometric Matching Service* has not been collected for the purpose of identifying individuals travelling under more than one identity or sharing the same ID document, but rather for purposes such as checking the preconditions for being granted a visa for a short-term stay in a Schengen country. The interoperability regulations react to this by defining rules for transferring and using the data.[32] Nevertheless, this is a completely different purpose compared to that for which the data had been initially collected. The interoperability regulations define new purposes meant to justify the combination of information included in the policing and migration databases.[33] However, these purposes are only defined in a very general and broad manner, which makes them highly problematic in the perspective of purpose limitation.

3.4 Proportionality: Interoperability as a new variation of data retention

Interoperability also raises questions of proportionality. The meta-functions established with the interoperability regulations use data of all individuals stored in one of the

---

[31] *See also* European Data Protection Supervisor, *supra*, n. 27, at 11 ff. and FRA (European Union Agency for Fundamental Rights), *Interoperability and Fundamental Rights Implications. Opinion of the European Union Agency for Fundamental Rights* 10 ff. (Vienna: FRA 2018).

[32] *See* Arts 28 to 35 Regulation (EU) 2019/818 for the CIR.

[33] *See* the general objectives and specific purposes defined, Art. 2 (objectives) and e.g. Art. 20 Regulation (EU) 2019/818.

databases integrated into the interoperability framework, including all third country nationals entering the EU. This means that the interoperability tools will massively use data of individuals who are neither related to any crime nor travelling with a false or more than one identity. Therefore, the interoperability tools can be conceived as a new variation of data retention. Compared to the retention of communication meta-data, the interoperability tools for policing and migration databases create additional risks for the individuals concerned. False hits can have serious consequences, such as the refusal of entry to the EU's territory or even an arrest.

The data stored in the *Biometric Matching Service*, the *Common Identity Repository* and in the *Multiple-Identity Detector* are retained in these systems for the very general purpose that individuals might use false identities. However, only a very minor part of the individuals concerned will ever use false identities. The only limitation for this specific variation of data retention defined in the interoperability regulations is the link to the storage of the data in the underlying databases. Erasure in all AFSJ databases will lead to automated erasure in the interoperability tools.[34] However, against the backdrop of the *Court of Justice of the European Union* (*CJEU*) judgments on this issue, the extent of data retention foreseen in the interoperability package remains highly problematic in the perspective of Articles 7 and 8 CFR.[35]

3.5 Data quality and accuracy: the risk of false hits

The quality of the data to be processed in the interoperability framework has a double impact. Accurate data reduces the risk of false hits that may have serious consequences for the individuals concerned. From the perspective of the police and other agencies involved, data accuracy reduces the risk of wasting time with investigations based on false or outdated information.

For the interoperability framework, this leads to additional regulatory challenges: How to make sure that outdated data is really removed from the databases? What will happen to data after it has been transferred to other law enforcement agencies? Will all the recipients of data be effectively informed if data must be updated or is due to be erased?

The answers delivered by the interoperability regulations remain vague: They transfer to eu-LISA the task to 'implement mechanisms for evaluating the accuracy of the shared BMS, common data quality indicators, and the minimum quality standards for storage of data in the SIS, Eurodac, ECRIS-TCN, the shared BMS,

[34] Articles 15 and 35 Regulation (EU) 2019/818.

[35] CJEU, cases C-293/12 und C-594/12, judgment of 8 Apr. 2014 (Digital Rights Ireland and others); cases C-203/15 and C-698/15, judgment of 21 Dec. 2016 (Tele 2 Sverige AB and others).

and the CIR'.[36] By contrast, the regulations do not include any new or more concrete approaches contributing to the implementation of data accuracy.

3.6 Privacy by design left to eu-LISA

The interoperability regulations leave the final decision about the interpretation of false or double identities detected by the automated interoperability tools to manual verification by the Member States' authorities.[37] This is an important double-check, recognizing that decision-making cannot be purely automated where fundamental rights are affected.

Beyond this intervention of humans, many data protection solutions are based on rules that have to be applied by the individuals responsible for the data processing. This leads to risks related to the 'human factor' – individuals may misunderstand or neglect rules and duties. Therefore, shortcomings are likely to occur, for example for the erasure of outdated entries in the databases and in the interoperability tools.

By contrast, *privacy by design* and *privacy by default* as it is required by general EU data protection law[38] shift the responsibility for correct data processing from the individual users to the technical design of the system. For the interoperability of policing and migration databases, technical approaches could help to avoid misuse of data and make sure that fundamental data protection principles are observed. However, the interoperability regulations remain vague in this respect.[39] They foresee automatic deletion of data once the retention period has expired without specifying how this will be implemented technically.[40] Thus, if and how *privacy by design* and *by default* will be applied is left to the implementation by eu-LISA.

3.7 Interfaces between database interoperability and network-based information sharing

Another data protection problem is related to the interface between centralized AFSJ databases and network-based information sharing: Once standardized data has been transferred automatically with the help of centralized databases, the recipients will be responsible for what they do with this data and decide who has access.[41] This is also the case for information on multiple or false identities that officers working in police and other agencies will receive from the interoperability tools. Will they really

---

36 Article 37 (2) Regulation (EU) 2019/818.
37 Article 29 Regulation (EU) 2019/818.
38 Article 25 Regulation (EU) 2016/670 (GDPR).
39 *See also* European Data Protection Supervisor, *supra* n. 28, at 18 ff.
40 For example, Art. 23 Regulation (EU) 2019/818.
41 *See* Arts 29 to 34 Regulation (EU) 2019/818.

respect the rules of purpose limitation? Will they be informed about outdated information and remove it from all their files, including paperwork?

This adds to the risks related to interoperability. Interoperability includes more data in searches and will therefore probably lead to more 'hits'. Investigation data stemming from EU databases or directly from those agencies who hold the information, often with sensitive content, may then be spread (in a legally grey zone) outside the databases by informal networks and used elsewhere. Purpose limitation and updating the data in all places where it has been transferred to, in cases of errors or outdated data, will therefore become more difficult – if not impossible.

In conclusion, the legal framework established – with the interoperability regulations will hardly be able to regulate data protection and privacy in a way that assures a high level of protection for fundamental rights. As third country nationals are the biggest group of individuals concerned by the interoperability tools, practical hurdles for access to justice will make court cases less likely to occur for these tools. Interventions by the European Parliament, data protection authorities, and civil society watchdogs will remain necessary in order to raise the privacy standards for the interoperability of databases to an adequate level.

4 ENHANCED TRANSPARENCY AND INTEROPERABILITY OF ACCOUNTABILITY MECHANISMS AS A RESPONSE TO THE INTEROPERABILITY OF DATABASES?

The fast development of AFSJ databases and the now established interoperability tools will require increased and innovative accountability and data protection mechanisms. These may be related to *privacy by design* approaches and to more comprehensive coordination of accountability mechanisms beyond data protection, including civil society.

The use of data for other than the initial purpose makes data processing less transparent. In addition, individuals will be typically affected by the impact of the interoperability tools in situations that are mostly not transparent for them: background checks for visa applications, refusal of entry for third country nationals, data base queries in a police stop situation, etc.

In this respect, the European Parliament, during the legislative procedure, successfully added an interesting element to the regulations: A web portal will be 'established for the purpose of facilitating the exercise of the rights of access to, rectification, erasure or restriction of processing of personal data'.[42] This approach could be much further developed. The transparency rules as they have now been established still rely upon the initiative of the individuals concerned to actively ask

[42] Article 49(1) Regulation (EU) 2019/818.

for information about their data processed in the interoperability tools. However, especially for the non-EU citizens massively concerned by the new instruments, this is not likely to occur.

Transparency could therefore better be assured by rules defining pro-active information duties – facilitating access to information – for example about the purposes for which the data can be stored and processed and about when it will be erased.

The respect of the citizens' fundamental rights could also be strengthened by additional and innovative accountability mechanisms. The risks to fundamental rights posed by interoperability may at least partly be compensated by coordination of the accountability mechanisms. These mechanisms are meant to prevent, for example, arrests going back to false hits and human rights violations that might follow from the enhanced availability of the data.

The general EU data protection law contributes to the coordination of the data protection authorities' work and can streamline and increase the standards to some degree. The *European Data Protection Board*[43] has been attributed a number of tasks and responsibilities not only regarding the GDPR, but also the coordination of data protection for policing and criminal justice.[44] The interoperability regulations also foresee cooperation between the EDPS and the Member States' data protection authorities.[45] Cases to be decided by the CJEU will probably also contribute to harmonizing data protection standards and potentially lead to higher European standards due to the CJEU's *effet utile* doctrine – as long as the individuals concerned manage to circumvent the hurdles that may prevent them from access to the Court, which constitutes a limitation especially for third country nationals for whom it will be a challenge to open a lawsuit against an unlawful decision based on the interoperability tools.

5 CONCLUSION AND OUTLOOK

This article has shown that the interoperability of AFSJ databases, foreseen by Regulations 2019/817 and 818 as they were passed in May 2019, may be framed as an understandable reaction to cases in which highly dangerous individuals managed to travel undiscovered to and inside the EU with the help of multiple or false identities. However, while the intended interoperability of databases may contribute to preventing dangerous individuals from preparing serious crimes, the interoperability tools also lead to a new variation of massive preventive data retention. Technical and legal approaches limiting the risks that interoperability constitutes for fundamental rights are still underdeveloped.

---

43 Established by Arts 68 ff. Regulation (EU) 2016/679 (GDPR).
44 By Art. 51 Directive (EU) 2016/680.
45 Article 53 Regulation (EU) 2019/818.

The implementation of the IT infrastructure for interoperability, including the *European Search Portal*, the *Biometric Matching Service*, the *Common Identity Repository*, the *Multiple Identity Detector*, as well as the communication between these tools and the Member States' and other EU agencies' IT infrastructure, is complex. Delays are likely to occur before these tools become fully operational. This is not unusual for complex European IT projects. The technical implementation of the first- and second-generation *Schengen Information System* took much longer than initially scheduled, and this is likely to happen again for the interoperability tools. The *Justice and Home Affairs* (JHA) Council therefore currently keeps this topic on the agenda for each regular meeting. Nevertheless, the SIS and other major IT projects that have been implemented in the past, demonstrate that new IT tools will be ready at some point in time. Then, adequate legal and technological solutions for a fundamental rights-friendly implementation will become even more important. The very general – references to fundamental rights and non-discrimination in Regulations 2019/817 and 818 are not more than a declaration of intent that will need to be filled with more substance.[46]

Another issue has been often neglected in recent debates on how to react effectively to new security threats: The massive growth of law enforcement powers that interoperability and other security initiatives have led to in recent years suppose that the EU and its Member States are based upon solid rule of law systems, but is this really assured? Recent developments in EU countries such as Hungary and Poland, as well as periods of populist governments in Austria, Italy, and other Member States, demonstrate the risks to the independence of the judiciary and for the rule of law in general, in relation to governments composed of representatives from populist parties. Can it really be taken for granted that these governments will respect and protect the fundamental rights of all citizens? What might happen if populist governments start to abuse the massive surveillance capacities that have been established for policing and transnational security cooperation over the past decades to prosecute political opponents and to silence critique by journalists and citizens? Does the European Union need a new variation of an 'emergency brake' to exclude Member States from access to AFSJ databases and to the interoperability tools if their rule of law system is deficient?

If the European Commission has started to complement or even replace the *Area of Freedom, Security and Justice* with an 'effective and genuine Security Union'[47] – skipping over freedom and justice (?), there is a risk that fundamental rights will lose importance in a European Union shaped by the massive extension of new tools such as those foreseen by the interoperability regulations.

---

[46] Article 5 and Recital 79 of Regulation 2019/818; *see also* the suggestions by the FRA, *supra* n. 31, at 13 ff.

[47] European Commission, *Communication from the Commission to the European Parliament, the European Council and the Council: Twelfth Progress Report Towards an Effective and Genuine Security Union*. Brussels. Brussels: COM(2017) 779 final.