European University Institute
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

EUI WORKING PAPERS

RSCAS 2019/15
Robert Schuman Centre for Advanced Studies

Interoperable Law Enforcement Cooperation Challenges in the EU Area of Freedom, Security and Justice

Francesca Galli

European University Institute

Robert Schuman Centre for Advanced Studies

Interoperable Law Enforcement

Cooperation Challenges in the EU Area of Freedom, Security and Justice

Francesca Galli

EUI Working Paper **RSCAS** 2019/15

ISSN 1028-3625

Printed in Italy, February 2019
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu/RSCAS/Publications/
www.eui.eu
cadmus.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Brigid Laffan, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and *ad hoc* initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

Abstract

At present EU institutions and agencies as well as national legislators have ambitious agendas on law enforcement authorities' access to interoperable information systems, which have become a defining feature of the AFSJ. They are the most advanced form of information exchange, conferring direct information access to competent authorities. Interoperable information systems are meant for the exchange of raw material for investigation purposes, which at a later stage could become evidence at trial. Interoperable information systems challenge existing cooperation dynamics and redefine the role of the actors involved. In fact, it is questionable whether mutual recognition and harmonisation, which have been considered the cornerstone of judicial cooperation in both civil and criminal matters for many years, can describe alone integration dynamics in law enforcement cooperation, particularly with reference to information sharing. This paper appraises whether, and to what extent, law enforcement access to and use of interoperable information systems constitute new modes of law enforcement cooperation in the EU AFSJ. It closely considers actors and/or factors which either hinder or foster such developments to assess what would be the implications of such a paradigm change in information management.

Keywords

Information management, interoperability, European Union, Area of Freedom Security and Justice, law enforcement.

Introduction

Terrorist attacks and the pressure from migration flows keep information-sharing at the top of EU priorities in the Area of Freedom, Security and Justice (AFSJ).[1] The information revolution provides criminal organisations with new tools, challenging traditional means of investigation. Law enforcement authorities therefore insist on the need to exploit technological advances which streamline information-sharing and interoperability to effectively fight serious transnational crime.

At present, EU institutions and agencies as well as national legislators have ambitious agendas regarding the access by law enforcement authorities to interoperable information systems. These have become a defining feature of the AFSJ. They are the most advanced form of information exchange and they allow competent authorities direct access to information. Interoperable information systems are created for the exchange of raw material for investigation purposes, which at a later stage could become evidence at trial.

Interoperable information systems challenge the existing dynamics of cooperation and redefine the roles of the actors involved. In fact, it is questionable whether mutual recognition and harmonisation, which have been considered the cornerstone of judicial cooperation in both civil and criminal matters for many years, can alone describe the dynamics of integration in law enforcement cooperation when it comes to information sharing.

This working paper appraises whether, and to what extent, law enforcement access to and use of interoperable information systems constitute new modes of law enforcement cooperation in the EU AFSJ. It examines the actors and/or factors which either hinder or facilitate these developments to assess the implications of this paradigm change in information management.

After a short overview of the main features of interoperability (section 1), the paper addresses whether and how the establishment and functioning of interoperable information systems actually or potentially redefine the existing distribution of tasks between the EU and the Member States (section 2) and among competent authorities of different kinds, including private actors (section 3). Having identified several common trends in the dynamics of cooperation, the paper draws some preliminary conclusions.

1. Interoperable information systems

Information systems or databases, as they are commonly labelled, are information management arrangements or tools which result in either specific software, IT systems or organizational infrastructures supporting different kinds of inter-jurisdictional information-sharing activities. They establish procedures for the exchange of information between organisationally independent bodies, both from the Member States and at the EU levels, with a relatively high level of information integration. Legal arrangements for information management create multiple horizontal interactions between authorities in different Member States and also vertical interactions between national authorities and EU agencies.[2] The inputs come from executive actors at different levels.

---

1 See F. Boehm, Information sharing and data protection in the Area of Freedom Security and Justice (Springer, 2012).

2 Ballaschk describes the interoperability between three different kinds of network: vertical networks, which are structured networks established by a formal legal arrangement (e.g. EU agencies such as Europol); horizontal networks, which are characterized by a certain degree of informality (e.g. Prüm cooperation); and intermediate networks, which are either established by a formal legal arrangement but have no hierarchical structure or have a hierarchical structure but no formal legal basis (e.g. SIS, VIS, Eurodac). See J. Ballaschk, *Interoperability of Intelligence Networks in the European Union: An Analysis of the Policy of Interoperability in the EU's Area of Freedom, Security and Justice and Its Compatibility with the Right to Data Protection*, PhD thesis, University of Copenhagen 2015 [still unpublished].

Such activities have intensified over the years. At first they consisted of *ad-hoc* exchanges of information in the form of mutual legal assistance, but then the development of more powerful means of computer-based information exchange led increasingly to the establishment of more structured forms of information networks in a wide spectrum of EU policy areas.

1.1. An undefined buzzword

Interoperability has existed for a long time, well beyond the realm of security and migration policies.[3] It has also become a buzzword in European policy debates on the future of the digital economy. In its Digital Agenda, the EU Commission portrays a lack of interoperability as one of the seven "most significant obstacles" to the "virtuous cycle" of digitalization.[4]

However, one of the difficulties in discussions on interoperability is the absence of a clear shared definition. Wallwork and Baptista propose a holistic notion of interoperability "as an umbrella beneath which may exist many disparate yet complementary definitions, according to a given perspective or layer of abstraction."[5] Interoperability is, in fact, a complex issue involving several layers and dimensions. Each definition therefore bears a major risk of strong bias or generalization resulting from a single perspective.

For the purpose of this working paper, interoperability can be tentatively described as the ability of an information system to exchange data and enable information-sharing with a technically different information system and to use the information that has been exchanged.[6] This definition does not even try to address how information may then be used. In the EU, in fact, although forms of interoperability between Member State authorities and EU agencies differ considerably from one policy area to another, what they all have in common is that the essence of the procedural cooperation consists in the establishment, generation and sharing of information irrespective of its eventual use in making decisions.

Interoperability is not a source of concern per se and could have a number of positive implications. From the perspective of EU policy-makers, it can improve the efficiency of Europe-wide information-sharing tools by providing the technical processes, standards and tools that allow EU information systems to work better together. In the AFSJ, it has the asset of potentially enhancing the effectiveness of the fight against serious crime, including terrorism. It can in fact provide authorised users (such as police officers, migration officials and border guards) with faster, seamless and more systematic access to the information they need to do their jobs.[7] The establishment of such information systems is therefore a key element in the AFSJ, and it also facilitates exchanges with third countries such as the US.

As the High-Level Expert Group on Interoperability argues, interoperability does not mean pooling all data or collecting additional categories of information. It does not entail data registered in one system being automatically shared across all other systems. Interoperability is about a targeted and intelligent way of using existing data to the best effect while at the same time ensuring full respect for fundamental

---

3 A. Pelizza, "Developing the Vectorial Glance. Infrastructural Inversion for the New Agenda on Government Information Systems" (2016) *41(2) Science, Technology, & Human Values* pp. 298-321; W. Kerber and H. Sweitzer, "Interoperability in the digital economy," 8 (2017) *JIPITEC* 39; J. Palfrey and U. Gasser, The promise and perils of highly interconnected systems (Basic books, 2012).

4 See EU Commission, *A Digital Agenda for Europe*, COM(2010)245 fin., 19 May 2010, p. 3.

5 A. Wallwork and J. Baptista, "Undertaking interoperability" in J. Backhouse (ed.), *Structured account of approaches to interoperability*, Ch. 4, Report D4.1, Future of identity in the information society (FIDIS), 2005, pp. 19-24.

6 See J. Palfrey and U. Gasser, *Interop*, 2012, p. 5; and the *Standard Glossary of Software Engineering Terminology* (IEEE 610) of the Institute of Electrical and Electronics Engineers.

7 Communication from the Commission to the European Parliament, the European Council and the Council, *Seventh progress report towards an effective and genuine Security Union, Strasbourg*, 16.5.2017 COM(2017) 261 final.

rights, including privacy and data protection requirements. In particular, it is about better protecting the EU's external borders, improving migration management and enhancing internal security for the benefit of all citizens.[8]

There is a clear attempt to present interoperability as a mere technical issue, whereas it is a sensitive matter of legal concern and also a crucial political choice.[9] At least, the technical dimension of interoperability can and should be disconnected from its other dimensions.[10] Such initiatives are inspired by the conventional wisdom in the security field that 'more is better' and that a proliferation of (connected) databases would enhance security.

1.2. The Commission Proposals

In this context, in December 2017 the Commission presented two proposals on the interoperability of information systems in the AFSJ.[11] By virtue of the proposals, law enforcement authorities would be able to check whether data on an individual is stored in one of six EU databases (VIS, SIS II, Eurodac, the Entry/Exit System (EES), ETIAS and the proposed ECRIS-TCN). This access would be based on four mechanisms. First, the European Search Portal (ESP) would enable users to detect whether information on an individual third-country national is available in one of the EU large-scale databases. Second, the use of a shared biometric matching service (shared BMS) would enable a comparison of biometric data (fingerprints and facial images) from several central systems (in particular, SIS, Eurodac, VIS, the future EES and the proposed ECRIS- TCN system). Third, a common identity repository (CIR) would be used for storing the biographical and biometric identity data of third-country nationals recorded in Eurodac, VIS, the future EES, the proposed ETIAS and the proposed ECRIS-TCN system. Finally, a multiple-identity detector (MID) would enable verification of whether the queried identity data exists in more than one system, to identify frauds.

The intertwining of legal frameworks and instruments which have established different information systems and given access to data to either or both national law enforcement authorities and EU agencies makes the Commission project very ambitious.[12]

There are still a number of worrisome elements to be considered and the proposals have been critically received by various organisations, including the European Data Protection Supervisor (EDPS)[13] and the Fundamental Rights Agency (FRA).[14] According to the Explanatory Memorandum,

---

8 High-level expert group on information systems and interoperability, Report, 2017.

9 See P. De Hert and S. Gutwirth, "Interoperability of police databases within the EU: An accountable political choice" (2006) 20 (1-2) *International Review of Law, Computers and Technology* 21-35; V. Mitsilegas, "The borders paradox: the surveillance of movement in a Union without internal frontiers," in H. Lindahl (ed.), *A right to inclusion and exclusion?* (Hart, 2009), pp. 34-63, at p. 56.

10 This way of proceeding was already criticized by the European Data Protection Supervisor with reference to the first concrete discussions on interoperability in 2005. See EDPS, *Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability* (COM(2005) 490 final), Brussels, 28 February 2006.

11 *Proposal for a regulation 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, COM(2017)793, 12 December 2017; Proposal for a regulation on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration),* COM(2017) 794 final, 12 December 2017.

12 The Commission published amended versions of the proposaed regulations on interoperability. See *Amended proposal for a Regulation on establishing a framework for interoperability between EU information systems (borders and visa)*, COM 478, 13 June 2018 and *Amended proposal for a Regulation on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)*, COM 480, 13 June 2018.

13 European Data Protection Supervisor, *Opinion 4/2018 on the Proposals for two regulations establishing a framework for interoperability between EU large-scale information systems*, 16 April 2018.

14 European Union Agency for Fundamental Rights, *Interoperability and Fundamental Rights Implications*, July 2017.

the 2017 proposals will not change the purpose, content or structure of the five relevant databases: the relevant identity data would be stored in the Common Identity Repository but would continue to 'belong' to the underlying systems that recorded them. However, a general feature of these initiatives is the link between data sets which until then had been stored and used for sector-specific purposes. The proposed interoperability would enhance this situation even further, given that the databases would be accessible to an ever-increasing number of actors for a growing number of purposes. This is an obvious challenge for data-protection principles, especially purpose limitation, data minimisation, data security and the clear allocation of data responsibilities. Additional legal issues concern the acceptable degree of, or timeframe for, an informal development of innovative information exchange mechanisms, networks or supervisory authorities and the effectiveness of administrative or judicial appeal and review procedures.[15]

1.3. Interoperability in practice

The Member States are striving for an almost unlimited and flexible functionality of the AFSJ databases. The new Entry/Exit System (EES),[16] the European Travel Information and Authorization System (ETIAS) regulations[17] and the amended proposals on SIS II[18] already provide a picture of how interoperability could work in practice.

The EES is a new database where the entry and exit records of third country nationals (TCNs) who enter the EU for a short stay are recorded. The data stored include both alphanumeric and biometric data (facial image and fingerprints). By virtue of Art. 8 of the regulation, the EES and Visa Information System (VIS) are interoperable.

The ETIAS mirrors existing programmes such as the US's ESTA.[19] It requires TCNs who are visa-exempt to complete an online form with their alphanumeric data in advance. This is used to screen the applicant for security, health and illegal immigration risks through several information systems, e.g. SIS II, and also through a newly established watchlist at EUROPOL. The ETIAS will include a repository of data in common with the EES and the automatic communication of certain newly entered alerts in the SIS II, e.g. on entry bans for TCNs, for a cross-check with the ETIAS. In addition, article 11 of the ETIAS regulation refers in general terms to interoperability with other EU information systems and Europol data.

There are several proposed enhancements to the SIS II, which contains alerts on entry bans for TCNs and on people and objects wanted for law-enforcement purposes. Amongst others, the amendments

---

15 See D. Curtin, "Security of the interstice and inter-operable data sharing: a first cut," in S. Carrera and V. Mitsilegas, constitutionalising the Security Union: effectiveness, rule of law and rights in countering terrorism and crime, Brussels: CEPS, 2017, pp. 65-72.

16 *Regulation (EU) 2017/2226 of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011*, *OJ* L 327/20.

17 *Regulation (EU) 2018/1240 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS)*, 12 September 2018, *OJ* L 236/1.

18 *Proposal for a Regulation on the use of the Schengen Information System for the return of illegally staying third- country nationals*, COM(2016) 881 final, 21December 2016; *Proposal for a Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006*, COM(2016) 882 final, 21 December 2016; *Proposal for a Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU*, COM(2016) 883 final, 21 December 2016.

19 The Electronic System for Travel Authorization, or ESTA, is an online application system developed by the United States government to pre-screen travellers wishing to visit the US. See https://apply-travel.us.com

would enable biometric cross-checking with the biometrics stored in the SIS II; synergy with other biometric systems in terms of the biometric data to be processed; a possible shared biometric system with other information systems for face and fingerprints searches; and an interconnection with Interpol.

***

It clearly emerges that interoperability has become a very dynamic field of EU policy but sometimes there is a lack of consistency and clear indications of the use of the instruments developed. Law enforcement authorities are confronted with a plurality of legal bases, channels, procedures and tools for different categories of information.

The next two sections explore the impact of interoperability on competence, which in broad terms is understood to encompass the concepts of 'jurisdiction' and 'task.' First, information-sharing via interoperable networks challenges the existing dynamics of integration, including both harmonisation and the principle of mutual recognition. Second, interoperability leads to a blurring of information-sharing tasks between several law enforcement actors for different purposes, and also an increasing involvement of private actors.

2. Interoperable information systems and integration dynamics

The concept of mutual recognition, in combination with the harmonisation/approximation of substantive and procedural law, has been considered a cornerstone of judicial cooperation in both civil and criminal matters for many years. However, it is questionable whether mutual recognition and harmonisation can alone describe the dynamics of integration in law enforcement cooperation, particularly with reference to information-sharing.

2.1. Approximation

Approximation of criminal law has various functions in the establishment of the AFSJ. First, it enables smooth judicial cooperation through various mechanisms based on mutual trust, particularly mutual recognition. Second, it facilitates the fight against crime: approximation is necessary to effectively deal with serious crime as otherwise criminals may take advantage of differences between criminal justice systems to identify less effective ones as safe havens (a kind of 'forum shopping'). Finally, it fulfils the crucial so-called 'shield function' (as opposed to the 'sword function') of criminal law, which corresponds to the commitment of the Member States to respect and protect individual rights.[20] It ensures the protection of individual rights and equal treatment before the law. Maintaining the existing differences between national frameworks is undesirable in the light of the common objective of a cohesive fight against serious crime. In addition, approximation has a clear added value: it can indirectly ensure comparable minimum standards of data protection throughout the continent because an EU instrument can require Member States to define national provisions in such a way as to respect minimum standards of individual rights protection, most importantly data protection in data retention and sharing. For the purpose of an enhanced protection of individual rights, approximation of national provisions would also indirectly avoid the risk of a perilous situation where data sharing occurs in a legal void, should there not yet be national provisions on the matter.

Of course, approximation of national provisions does not guarantee that their practical application will follow the same or similar standards. The variety of legal cultures is likely to cause significant differences (e.g. concerning understanding of the function of statutory provisions on the one hand and judicial decisions on the other, or the discretion of law enforcement agencies at the procedural level).

[20] See A. Weyembergh, *Le rapprochement des législations, condition de l'espace pénal européen et révélateur de ses tensions* (Éditions de l'Université de Bruxelles 2004); A. Weyembergh, 'The Functions of Approximation of Penal Legislation within the EU,' 12 *MJECL* 2 (2005), p. 149-172.

However, the entry into force of the Lisbon Treaty has improved the situation quite significantly as the approximation of criminal law and procedure becomes a treaty objective. In addition, the TFEU now provides a clearer legal basis for the harmonisation of substantive criminal law, although many of the instruments for this were adopted before the existence of this legal basis. When it comes to the harmonisation of criminal procedural law, the new and clearer legal bases provided by the Lisbon Treaty have deeply impacted the field, as most instruments have been adopted after 1 December 2009. At the same time, the CJEU is likely to have a moderating and facilitating effect.[21]

2.2. The principle of mutual recognition

In its 1999 Tampere Conclusions, the European Council "endors[ed] the principle of mutual recognition which [...] should become the cornerstone of judicial co-operation in both civil and criminal matters within the Union."[22] The adoption of instruments was very much in focus in the aftermath of Tampere, but newer instruments, such as the EIO Directive, have been adopted since the Lisbon Treaty's entry into force.

In the AFSJ, successful operation of the principle of mutual recognition implies that Member States must trust each other when it comes to complying with fundamental rights.[23] This means that the principle of mutual recognition presupposes mutual trust and comity among national judiciaries.[24]

In Opinion 1/2013, the CJEU inferred that when implementing EU law Member States are required to presume that fundamental rights have been observed by the other Member States. This presumption imposes two negative obligations on the Member States. First, they may "not demand a higher level of national protection of fundamental rights from another Member State than that provided by EU law."[25] Second, "save in exceptional cases," Member States are prevented from "check[ing] whether that other Member State has actually, in a specific case, observed the fundamental rights guaranteed by the EU."[26]

The relationship between mutual recognition and approximation is sensitive.[27] Both instruments aim for a common AFSJ where judicial decisions can move freely across borders and where EU Member States can work together in order to prevent and punish crime. Reliance on the principle of mutual recognition was seen as the most practicable avenue to overcome the opposition of some Member States to the harmonisation of substantive aspects of their criminal laws, as the principle would strike a balance between 'unity and diversity.' On the one hand, the principle of mutual recognition leaves the substantive criminal laws of the Member States largely untouched. On the other hand, judicial

---

21 See A. Weyembergh, "Approximation of substantive criminal law: the new institutional and decision-making framework and new types of interaction between EU actors" in F. Galli and A. Weyembergh (eds.), *Approximation of substantive criminal law: the way forward* (Editions de l'Université de Bruxelles, 2013).

22 Presidency Conclusions, Tampere European Council, 15-16 October 1999, para. 33.

23 For an in-depth analysis of the principle of mutual recognition, see S. Peers, "Mutual recognition and criminal law in the European Union: Has the Council got it wrong?" (2004) 41(1) *Common Market Law Review* 5; V. Mitsilegas, "The constitutional implications of mutual recognition in criminal matters in the EU" (2006) 43(5) *Common Market Law Review* 1277; A. Suominen, *The principle of mutual recognition in cooperation in criminal matters – A study of the principle in four framework decisions and in the implementation legislation in the Nordic Member States* (Intersentia, 2011) 51–55.

24 L. Bay Larsen, 'Some Reflections on Mutual Recognition in the Area of Freedom, Security and Justice,' in P. Cardonnel, A. Rosas and N. Wahl (eds.), *Constitutionalising the EU Judicial System: Essays in Honour of Pernilla Lindh* (Oxford: Hart Publishing, 2012) at 148.

25 Opinion 2/13, EU:C:2014:2454, para. 192.

26 Ibid. For a comment, see M. Bossuyt, "The principle of 'mutual trust' in Opinion 2/13" and E. Bribosia, "Fundamental rights and mutual trust in the European Union – the story of a clash foretold?" in *The EU fundamental rights landscape after Opinion 2/13*, Maastricht faculty of Law Working Paper, 2016.

27 A. Suominen, "The Sensitive Relationship Between the Different Means of Legal Integration: Mutual Recognition and Approximation" in C. Brière and A. Weyembergh (eds.) *The Needed Balances in EU Criminal Law: Past, Present and Future* (Hart Publishing, 2018), pp. 165–184.

cooperation prevents criminals from relying on free movement as a means of pursuing their activities with impunity. Instead of opting for total harmonization, one might conceive a situation "where each Member State recognizes the validity of decisions of courts from other Member States in criminal matters with a minimum of procedure and formality."[28]

The question is what degree of equivalence or approximation of standards is a precondition for mutual recognition.[29] In the AFSJ, the EU legislator not only has competence to facilitate the application of the principle of mutual recognition but may also specify a common level of fundamental rights protection for persons involved in judicial cooperation between Member States. In order to function, the principle of mutual recognition therefore requires a minimum level of harmonisation in relevant areas. This was explicitly recognised in the Lisbon Treaty itself: minimum rules concerning the admissibility of evidence, the rights of individuals in criminal procedures and the rights of victims of crime can be established to the extent necessary for the realisation of mutual recognition and police and judicial cooperation in criminal matters with a cross-border dimension (Article 82(2) TFEU).[30] By establishing a 'level playing field' for these aspects of criminal procedure, the Treaty facilitates the free movement of judicial decisions. A Member State is in fact more likely to recognise and enforce decisions issued in other Member States if the fundamental rights of the person(s) concerned are properly protected throughout the EU. With the entry into force of the Lisbon Treaty, the focus has shifted from the harmonisation of substantive criminal law, and mutual recognition, to the harmonisation of the procedural rights of the individual. In addition, the priority is to not create more instruments, either on mutual recognition or harmonisation, but instead to consolidate or codify existing instruments.[31]

Whereas mutual recognition is the cornerstone of judicial cooperation, law enforcement cooperation in criminal matters is characterised by a strong emphasis on the principle of availability. An information-sharing policy based on the principle of availability of and access to information first emerged in the 2004 Hague Programme, which insists on the significance of information exchanges between interoperable information systems and law-enforcement (including both national authorities and EU agencies) access to the information thereby retained, for both security and border management purposes.[32] The 2005 Treaty of Prüm implemented the Hague Programme in order to establish the highest possible standard of cooperation, in particular by means of the exchange of information.[33] Then, in its Communication of April 2016, the Commission set out its vision with regard to the interoperability of existing and future AFSJ information systems in more concrete terms.[34]

---

28 Mitsilegas, *European Criminal Law*, p. 116.

29 M. Möstl, "Preconditions and Limits of Mutual Recondition" (2010) 47 *Common Market Law Review* 406.

30 See also J. Ouwerkerk, Quid Pro Quo? A comparative law perspective on the mutual recognition of judicial decisions in criminal matters (Intersentia 2011).

31 See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'The EU Justice Agenda for 2020 – Strengthening Trust, Mobility and Growth within the Union,' COM(2014) 144 final, 11.3.2014.

32 European Council (2004). *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, 5 November 2004, *OJ*, C 53/1, 3 March 2005.

33 Also referred to as the Prüm Convention or the Schengen III Agreement, adopted outside the EU framework and later subsumed into the provisions of EU law for police and judicial cooperation by Council Decision 2008/615/JHA. See *Prüm Convention*, adopted 27 May 2005; *Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.* For a comment, see O. Sallavaci, "Strenghtening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange" (2018) 24 *Eur J Crim Policy Res* 219.

34 *Stronger and Smarter Information Systems for Borders and Security*, COM(2016) 205 final, 6 April 2016.

In particular, initiatives for the exchange of information are part of a broader EU 'information management policy' to improve shared knowledge of common threats[35] between competent national authorities, which is a core element in the fight against serious crime.[36] Reinforcing law enforcement cooperation within the EU has been one of the AFSJ's priorities, especially since the adoption of the 1999 Tampere Programme.

2.3. Alternative cooperation mechanisms?

Policy developments in the AFSJ have been characterized by a firm belief in the added value of approximation and mutual recognition. Taking the national legislation of the requesting state as the point of reference has increasingly become accepted in information-sharing via mutual assistance mechanisms in criminal matters. In addition, the approximation of national legislation in specific fields has fostered the underlying mutual trust required. The European Union is now practising and proposing in the AFSJ "alternative" cooperation mechanisms which do not aim at a formal harmonization or approximation of national provisions. The coordination of member states' policies and national law enforcement activities, particularly with reference to cross-border challenges, is entrusted to the exchange of information based on commonly agreed general principles and goals.

Interoperable networks, for instance, have developed in the form of "platform integration."[37] Thus, the security model of integration which emerges through the emphasis on interoperability fosters de-centred cooperation. More traditional models of European integration insist on the harmonization/approximation of legal provisions to common standards and the redistribution of competences and rights to the advantage of the supranational level. Interoperability allows the exchange of data and the sharing of information and knowledge among IT systems, while preserving significant distinctions. Technical platforms and information hubs function across national boundaries and across the traditional public-private divide, configuring a new form of 'platform integration'. This mode of information sharing does not imply the creation of an over-arching database: it connects existing systems of data storage while leaving them decentered and dispersed. It does not create new systems or competences. Actors of different sorts and at different levels (local, national, supranational are connected in a data-driven mode. Interoperability thus goes beyond thorny questions of common policing such as the issue of national security competence in the EU AFSJ.

Integration through interoperability raises different kinds of concerns. Most importantly, these seemingly technical systems for data exchange have significant implications on the restructuring of rights and responsibilities, which are dispersed, in the EU AFSJ. There is emphasis on the national level, where EU agencies/networks are meant to function merely as a hub. It is yet to be seen, though, whether this is just rhetoric to side-line sensitive discussions on supranationalism. This new form of integration gives EU agencies new roles and powers. EU agencies and networks identify datasets, make them interoperable and generate leads. These leads and analyses are in turn re-routed to national security officials and local police so that security interventions remain national and local.

How does interoperability interact with harmonisation and mutual recognition mechanisms? The interoperability of EU information systems can help to systematise law enforcement authorities' modalities of access to data that is required for the effective completion of their tasks across the EU and thus indirectly foster harmonisation across Member States in this respect. However, most of the time interoperability bypasses approximation concerns. It does not focus on similarities and differences

---

35 As required in the Preamble of Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences, *OJ*, L 253, 29 September 2005; European Council Conclusions, EUCO79/14, at para. 3.

36 European Council Conclusions, EUCO79/14, at paras. 10-11.

37 The metaphor aims to compare the current shape of EU internal security integration to the Platform Economy of Uber and AirBnB. See M. De Goede, *Draft paper on "Platform Integration"* presented at the Conference "From Justice and Home Affairs to Security Union," Florence, November 2017 [still unpublished].

among legal systems but has as its main goal to put in contact and make operative systems that would otherwise be separated.

Mutual recognition has so far mainly applied to judicial cooperation. Introducing the mutual recognition philosophy in the field of law enforcement cooperation would have important implications which will undoubtedly facilitate and expedite information exchanges.[38] Some authors suggest that there is no question at all of mutual recognition in this context.[39] Others argue, more convincingly, that there is a close connection between the principle of availability and the principle of mutual recognition.[40] In particular, implementing the principle of availability according to the mutual recognition idea would give a wholly different meaning to the right to request and the obligation to provide. However, this approach is very much linked to traditional mutual legal assistance mechanisms of cross-border information exchange. Interoperable information systems bypass or sideline the principle of mutual recognition. There is no request for information between a requesting national authority and a requested national authority, but a simultaneous interplay among the information systems of different actors feeding the system with data sets or searching for information. The principle of availability as originally conceived has equally been revisited.[41] Interoperability would entail the interplay between information systems and actors of different kinds, and not only a full availability of information between two Member States in the context of ongoing investigations.

The exclusion of national security from EU competence, by virtue of Article 4(2) TFEU, provides for an additional layer of complexity.[42] Interstate cooperation within the AFSJ is formally limited to police cooperation, whereas intelligence-sharing – revolving around national security issues – would not fall within the realm of EU competence. However, data are increasingly integrated into informal mechanisms of transnational governance,[43] which has allowed the development of instruments of cooperation in the AFSJ notwithstanding delicate issues of national sovereignty and EU competence.[44] Such mechanisms include the interoperability of networks and agencies and play a crucial role in policy-making and enforcement.[45] In this context, the exchange of intelligence information happens *de facto* in any case.

The fact that in many countries there is no distinction between the kinds of information that fall within the two different categories or which actors can access and share the information has accentuated this development.[46] Moreover, there is increasing blurriness in the traditional distinction between police authorities and intelligence services, which are often referred to as 'law enforcement authorities.' Most often, the concept of 'law enforcement' is defined in terms of finalities with reference to the nature of the activities involved. It therefore increasingly encompasses any authority which is competent to

---

38 See G. Vermeulen et al, *Availability of law enforcement information in the European Union. Between mutual recognition and equivalent right of access* (Maklu, 2005).

39 G. Vermeulen, "Mutual Recognition, Harmonisation and Fundamental (Procedural) Rights Protection," in M. Martin (ed.), *Crime, Rights and the EU: the Future of Police and Judicial Cooperation* (London, Justice, 2008) 94.

40 See V. Mitsilegas, *EU Criminal Law* (Hart Publishing, 2009), 117–18.

41 According to the Hague Programme, the principle of availability implies that "throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State."

42 Art. 4(2) TEU.

43 See M. Kleine, *Informal Governance in the European Union* (Cornell University Press, 2013).

44 C. Tange, "L'acteur policier entre structures formelles et informelles," in G. De Kerchove and A. Weyembergh (eds.), *L'espace pénal européen: enjeux et perspectives* (Éditions de l'Université de Bruxelles, 2002).

45 See D.-U. Galetta et al, "Information exchange in the European Administrative Union: An Introduction" (2014) 20(1) *European Public Law* 65.

46 See, e.g., C. Cocq, " 'Information' and 'Intelligence': The current divergences between national legal systems and the need for common (European) notions" (2017) 8(3) *NJECL* 352-373.

conduct a crime investigation or a criminal intelligence operation. This may include the exchange of information between police,[47] customs and even immigration services. These authorities can exchange information or intelligence directly as long as their activity has a link with crime and as long as they exchange the information or intelligence outside the evidence phase, which would otherwise require authorisation by an independent judicial authority. The notion of 'law enforcement' is thus linked to the use that is made of the information, not to the category of the body exchanging the information. If there is (suspicion of) a link with a criminal offence, then competent national authorities can exchange information for the purpose of preventing, detecting and repressing criminal offences.[48] Such interpretation broadens the scope of information-sharing, clearly also involving national security issues.

However, the sharing of competence prevents any approximation of national provisions defining the scope of information sharing. In order to overcome the limit of national security competence remaining in the realm of Member State actions, interoperability allows the approximation of criminal law with reference to intelligence-sharing to be bypassed. When presented as a technical means connecting existing networks, which would not require further adjustment, interoperability does not engage in discussions as to who are the 'competent authorities' or what is 'serious crime' at the EU level – elements which were deeply debated with reference to the design of a data retention directive well before its invalidation by the Court of Justice.[49] Member State practices in designating 'competent authorities' show huge discrepancies. This adds to the complexity of systems and hampers the control of data flows. In addition, this discrepancy might create uneasiness and distrust among the authorities involved. Not every police officer or prosecutor, for instance, might feel comfortable with exchanging information with political bodies in other Member States. Such distinctions also entail great differences in conditions of access, which are a major problem in the exchange of information within the EU (with/without judicial control). Stronger supranational control of the Member States' diverging practices of designating 'competent authorities' would be desirable and harmonization would have a great role in this respect.

Member State competences in national security matters will in the end become a shortcoming in the coherent and cohesive development of an EU data-management architecture, hampering the effectiveness of EU border and security policies. Without a treaty amendment there is, moreover, a risk that in this area it will not be possible to go beyond a form of platform integration, thus bypassing the added value of approximation in criminal law measures, which would bring about greater safeguarding of individual rights. In addition, it remains to be seen whether by virtue of Article 4(2) TEU any data-processing by a national security agency falls outside the scope of Article 16 TFEU, which provides a new horizontal legal basis for the drafting of EU instruments on data protection.

3. The reshuffling of responsibilities between different actors

Reinforced police and judicial cooperation is one of the most important tools for the establishment of the AFSJ as provided for by Title V TFEU. By virtue of Article 87 TFEU, the EU establishes police cooperation involving all Member State competent authorities, including specialized law enforcement authorities. One important aspect of police cooperation is the exchange of information among the

---

47 Taking into account the national differences in police forces among Member States, the definition of police has to be broadly interpreted. If the authority concerned is authorized by national law to prevent, detect or investigate criminal offences or criminal activities and to exercise authority and take coercive measures in the context of such activities, then it can be regarded as a police force.

48 See Article 2 Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU: a "'competent law enforcement authority' [is] a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities." [2006] *OJ* L 386/89.

49 F. Galli, "Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions" (2016) 23(3) *Maastricht Journal of European and Comparative Law,* 460.

network of EU agencies, bodies and Member State authorities on the basis of EU initiatives, administrative agreements or international treaties.[50] The direct exchange of information and intelligence between law enforcement authorities is encouraged through the principle of availability, the web of liaison officers and interoperability between data information systems. In this context, interoperability not only challenges existing integration dynamics and the sharing of competence between the EU and Member States but it also redefines the distribution of tasks between law enforcement authorities of different kinds and involves private actors in information-sharing.

3.1. Law enforcement authorities

According to the strict principle of separation of powers, the activities of intelligence services and police authorities in the prevention and investigation of crime were traditionally defined and distinct. There is, in fact, a profound difference in the purposes of the two bodies. The police, in the framework of their judicial function, have the task of gathering information in relation to specific offences for prosecution purposes; intelligence services do not have the objective of investigating offences but instead to recognise threats and to provide intelligence assessments to policy-makers. In this framework, intelligence information[51] is mostly secret, whereas police information is subject to judicial scrutiny during the investigation phase and potentially via cross-examination in court. When intelligence is collected and stored by several security actors at different levels of government, a mixed oversight regime may apply to diffuse arrangements.

There has been an evolution of the share of roles, competences and technological capabilities of intelligence services and law enforcement authorities. The means at the disposal of each actor for the prevention and investigation of serious crime are evolving so that the shares of tasks and competences have become blurred. Nowadays the distinction is not always clear, and this leads to problematic coordination and overlap.[52] Intelligence has also been given operational tasks. Law enforcement authorities have resorted to ever more sophisticated surveillance technologies and have been granted much more intrusive investigative powers to use them. In doing so, they have brought their modus operandi closer to that of intelligence agencies. A faith in technological solutions and the inherent expansionary tendency of surveillance tools partially explains this phenomenon. Surveillance technologies, in fact, are used in areas or for purposes for which they were not originally intended.[53]

Function creep is pervasive in the blurring of boundaries between policing and intelligence. Information-sharing and exchange does not in itself blur the institutional barriers between agencies, but the nature of the large-scale information-sharing activities being carried out does shed new light on the position of intelligence activities in the law enforcement domain. The resources spent on and the knowledge developed by such large-scale information-gathering and analysis are *de facto* changing police officers into intelligence actors or intelligence material users. The information exchange being

---

50 See A. Jonsson Cornell, "EU police cooperation post-Lisbon" in M. Bergström and A. Jonsson Cornell (eds.), *European Police and Criminal law cooperation* (Hart, 2014).

51 Intelligence information refers to "secret material collected by intelligence agencies and increasingly by the police to provide background information and advance warning about people who are thought to be a risk to commit acts of terrorism or other threats to national security." See K. Roach, "Secret evidence and its alternatives," in A. Mansferrer (ed.), *Post 9/11 and the State of permanent legal emergency. Security and Human Rights in Countering Terrorism* (Springer, 2012), pp. 179-200.

52 The distinction of roles and information sharing between intelligence services and law enforcement authorities with a view to preventing and combating terrorism has been much discussed and has also led to controversial case law in a number of EU countries, including the Netherlands. See J.A.E. Vervaele, "Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?" (2005) 1(1) *Utrecht Law Review* 1.

53 C. Cocq and F. Galli, "The catalysing effect of serious crime on the use of surveillance technologies for prevention and investigation purposes" (2013) 4(3) *NJECL* 256.

carried out by large-scale EU information management systems (e.g. SIS II, VIS, Eurodac, API, ECRIS, PNR etc.) is regularly facilitated horizontally, i.e. only *among* police personnel, but large-scale cross-border information management is progressively eroding the cultural boundaries between law enforcement and intelligence services.

The centralisation of information-sharing between intelligence services and law enforcement authorities and the increasing involvement of intelligence services in the criminal justice system may be very effective for security purposes. However, it is regarded as increasingly interfering with the right to privacy and the protection of personal data without an acceptable level of judicial scrutiny. In addition, intelligence services must only be accountable to the executive. The reshuffling of responsibilities within the law enforcement community therefore fosters a further shift to the executive or semi-executive branches of state power. Given the new role of intelligence in public-order activities and the investigative domain, one of the issues at stake is that of the relationship, yet to be defined, between the intelligence services and the judiciary.[54]

The two proposals on interoperability would potentially further extend access to non-law-enforcement information systems to a wide range of national authorities with diverse tasks, not excluding intelligence agencies. Such authorities are designated by the Member States, and the only common denominator concerning their mandate is the prevention, investigation, detection or prosecution of serious crime and terrorism.

3.2. Security and migration actors

EU initiatives enhancing access to information by law enforcement authorities therefore have a direct impact on the functional borders in the security domain. The intention of the Commission is to improve information exchange not only between police authorities but also between customs authorities and financial intelligence units and in interactions with the judiciary, public prosecution services and all other public bodies that participate in the process that ranges from the early detection of security threats and criminal offences to the conviction and punishment of suspects. The Commission has portrayed obstacles to the functional sharing of tasks as follows: "Compartmentalization of information and lack of a clear policy on information channels hinder information exchange,"[55] whereas there is, allegedly, a need to facilitate the free movement of information between competent authorities within Member States and across borders.

In this context, a controversial aspect of interoperability is that systems and processes are linked with information systems that do not serve law-enforcement purposes, including other state-held databases and ones held by private actors. With reference to the first category, the issue to address concerns the blurring of tasks between different law enforcement actors (police authorities, intelligence services, customs officers). In fact, a key aspect of the EU strategy on databases and their interoperability is an aim to maximise access to personal data, including access by police authorities to immigration databases and to personal data related to identification. This blurring has an impact on the applicable legal regime (in terms of jurisdiction) and also in terms of legal procedure (e.g. administrative/criminal). In fact, the purpose for which data are gathered, processed and accessed is crucial, not only because of data protection rules but because it links the information/data with a different stage of a procedure (either administrative or criminal) to which a set of guarantees are (or are not) attached, and thus has serious consequences for the rights of individuals (including access, appeal and correction rights). Neither legal systems nor legal provisions are fully compatible because they either belong to administrative or criminal law or because of a lack of approximation between Member State systems. Such differences

---

[54] See R. Orlandi, 'Attività di intelligence e diritto penale della prevenzione' and F. Sommovigo, "Attività di intelligence e indagine penale" in Illuminati, *Nuovi profili del segreto di Stato e dell'attività di intelligence* (Torino, Giappichelli, 2010).

[55] In May 2004, the European Commission issued a Communication to the Council of Europe and the European Parliament aiming at enhancing law enforcement access to information by law enforcement agencies.

also have an impact on the potential use of information: information used for identification purposes (the focus of customs officers at Frontex); or only for investigation purposes with no need to reach trial (the focus of intelligence actors); or for prosecution purposes (the focus of police authorities). Eventually, of course, the actors involved in the process have different impacts on the potential secret use of data, with consequent transparency concerns.

In addition, the different AFSJ databases have different purposes: while some purely implement migration policies (an administrative purpose) others implement police and judicial cooperation in criminal matters.[56] Legally and structurally different bodies equipped with different tasks exchange and transfer personal data within and outside the EU. Interoperability challenges the purpose limitation principle,[57] which is a fundamental protection against uncontrolled use and dissemination of information going beyond the realm of data protection.[58] In fact, data collected for one specific purpose may be transferred and used for other purposes completely unrelated to the original collection. The purpose limitation discussion refers to the general trend of blurring lines between security and immigration policies and objectives.

For instance, law enforcement access to VIS and Eurodac has been extremely controversial over the years.[59] Both databases were, in fact, established for purposes other than security, primarily as border management tools.[60] In the case of Eurodac, data should only be entered and accessed by national authorities in charge of handling asylum requests. However, as the first coordinated inspection by data protection authorities showed, in some member states Eurodac is operated partly or entirely by national police services.[61] The intended proposal to grant law-enforcement officers access to Eurodac may only formally allow what already takes place.

In addition, the interoperability between ETIAS and Europol data is a good example. Europol's information system encompasses individuals of interest to law-enforcement authorities, mostly serious criminals and terrorists. This, together with the prospective establishment of the future Europol watchlist – which will also be fed by the UN and international partners and continually matched against ETIAS applicants and those already granted authorization – signals an increasing role of Europol. The main EU law enforcement agency would therefore play, more or less indirectly, a major role in decisions relating to migration matters. While security is an important concern in migration, the intensity of checks and the growing number of authorities influencing border-management decisions is noteworthy. As the EDPS has noted,[62] ETIAS checks could be seen as more intrusive than the ones for Schengen visa applicants.

Finally, it is unclear how far the possible changes to the original purposes of individual databases would pass the legality, necessity and proportionality tests. Ultimately, in fact, a strict application of the

---

56 See E. Brouwer, "Legality and Data Protection Law: the forgotten purpose of purpose limitation" in L. Besselink *et al* (eds.), *The eclipse of the legality principle in the European Union* (Kluwer, 2003).

57 The purpose limitation principle has served as a key principle in data protection for many years. It consists of two elements: data must be collected for specified, explicit and legitimate purposes only (*purpose specification*); and data must not be further processed in a way that is incompatible with those purposes (*compatible use*). See M. von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws* (Nomos, 2018).

58 More broadly, in law enforcement cooperation the principle of purpose limitation guarantees that the issuing law enforcement authority does not use the information obtained for other purposes. The piece of information is labelled "for law enforcement use only" and, for instance, can neither be used for trial nor administrative purposes.

59 See European Data Protection Supervisor, EDPS (2007), EURODAC Supervision Coordination Group, Report of the first coordinated inspection, 17 July 2007.

60 See E. Brouwer, "Legal boundaries and the use of migration technology" in H. Dijstelbloem & A Meijer (eds.), *Migration and the technological borders of Europe* (Palgrave, 2011).

61 EDPS, 2007, p. 12.

62 EDPS, *Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS)*, 3/2017, 6 March 2017.

principle of proportionality would, for instance, imply a prohibition of routine access for law enforcement purposes to non-police/security databases, such as the VIS or Eurodac.

Interoperability establishes a link between formerly unrelated policy areas, such as the prevention of serious crime and border management. In addition, it fosters cooperation among actors of a completely different legal nature and vested with different powers, also thanks to the enhanced cooperation and coordination between law enforcement agencies of different kinds.

3.3. The 'agentification' of the AFSJ

The development of information networks for the implementation of EU policies has gone hand in hand with increases in the number and powers of EU agencies,[63] and also in their access to data stored in European information systems. The process of 'agentification' of EU administration was initiated two decades ago and has gained momentum ever since. In the AFSJ, mechanisms of informal governance in information-sharing afford significant discretion to security executives, including EU agencies. It is therefore not by accident that EU agencies are often charged with establishing and maintaining information networks in the EU.[64]

Agencies assist in the implementation of EU policies and provide research/scientific advice for the elaboration and implementation of legislation. A welcome development in regulatory functioning terms is that agencies now have the possibility of adopting decisions that are discretionary but legally binding. In addition, in terms of their independence, agencies have been portrayed as 'in-betweeners'[65] between Member States and EU institutions. In the realm of the AFSJ, the enhanced mandate of agencies which are part of the executive governance of security goes far beyond administrative support and often leads to them steering EU policies. Given the increasing 'agentification' of the AFSJ, there is therefore an additional layer of complexity in the actors involved in information-sharing, with consequent legality and accountability concerns.[66] This is not only the case of intra-EU exchanges but also involves the external dimension of the EU AFSJ and the possible transfer of data to third countries/agencies (e.g. Europol).[67]

In the EU multilevel system, two types of police information-sharing can be observed: centralised approaches in which databases play a major role and network-based approaches. A range of agencies have in fact been established that collect, analyse and operationalise police information and intelligence regarding strategically defined security threats.[68] Thus, in recent years, the centralised support infrastructure for policing has been streamlined by the transformation of multiple institutional settings

---

63 For the emergence of agencies in the integrated administration structure of the EU, see H. Hofmann and A. Turk, "Legal challenges in the move to an integrated administration" in Hofmann and A. Turk (eds.), *Legal challenges in EU administrative law* (Edward Elgar, 2009) 355-379; M. Chamon, *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration* (OUP, 2016).

64 See e.g. Art. 11 of Regulation (EU) no. 439/2010 of 19 May 2010 establishing the European Asylum Support Office, *OJ* L 132/11.

65 M. Everson et al (eds.), *EU Agencies in between Institutions and Member States* (Kluwer, 2014).

66 See e.g. M. Busuioc, D. Curtin and M. Groenleer, "Agency growth between autonomy and accountability: the European Police Office as a 'living institution'" (2011) 18(6) *Journal of European Public Policy* 848; S. Peers, "Governance and the third pillar: the accountability of Europol" in D. Curtin and R.A. Wessel (eds.) *Good Governance and the European Union: Reflections on Concepts, Institutions and Substance* (Intersentia, 2005), 253-276.

67 F. Coman-Kund, "The International Dimension of the EU Agencies: Framing a Growing Legal-Institutional Phenomenon" (2018) 23(1) *European Foreign Affairs Review* 97.

68 M. Den Boer, "Counter-terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis (2015) 30(2-3) *Intelligence and National Security* 402.

into formal EU agencies, such as Europol, Frontex and eu-LISA.[69] Inter-agency cooperation between AFSJ actors has led to the conclusion of agreements providing for mutual information exchanges. Moreover, during the migration crisis, and coupled with an alleged increase in terrorist attacks, the role of Europol and Frontex in 'knowledge production' has been fundamental in designing a security response. Both agencies are also lobbying Member States for an increase in their competences in border and security management, most importantly via interoperable databases, in the name of effectiveness.

Europol has played a leading role in the development of methods and instruments for reliable police information and intelligence exchanges on serious crime and terrorism over the years.[70] Its status, legal basis, competence and powers have evolved very quickly since its establishment in 1995.[71] The new Europol Regulation of May 2016[72] makes Europol more effective in collecting and analysing information and then sharing such analyses with the Member States. In addition, it enhances Europol's ability to access and retrieve information from Member State databases. The new legal framework allows Europol to provide more comprehensive support to competent national authorities involved in cross-border investigations.

Europol has developed from being an information hub to an increasingly (pro)active agency. In particular, it has had a growing impact on the exchange and analysis of information.[73] Its supporting and operational capacities have evolved, which can be explained by two factors. On the one hand, the agency has acquired maturity and experience over time and its databases have evolved to enhance the added value of the agency in cross-border cooperation. On the other hand, it benefits from major changes in the AFSJ such as an improvement of cooperation mechanisms and the harmonisation of Member State legislation.[74] The agency gathers information from competent authorities and shares it with EU Member States and third parties.[75] It also offers strategic and operational analysis.

Information is transmitted by the European National Units (ENU) – the liaison bodies between Europol and each competent national authority – to Europol SIENA (Secure Information Exchange Network Application). It is then stored for operational and strategic analysis purposes. For operational purposes, the Europol Information System (EIS) and the Analysis Work Files (AWFs) are the two databases containing personal data at the moment, with the AWFs containing the same data as in the EIS, namely on suspects, convicted criminals or persons for whom there are factual indications or reasonable grounds to believe that they will commit crimes that fall within Europol's competence, together with contacts, associates, witnesses, victims and informants. The spectrum of information is thus very broad and varied. AWFs are divided into two categories: terrorism and organised crime. In

---

69 The European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is a newly established EU agency to provide a long-term solution for the operational management of large-scale IT systems, which are essential instruments in the implementation of the asylum, border management and migration policies of the EU. See Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011, *OJ* L 286/1, 1.11.2011.

70 Europol has no control over the definition of the term 'information.' It may receive intelligence considered as such in some states and not in others. The expression 'exchange of information' by Europol must therefore be understood broadly.

71 Council Act of 26 July 1995 drawing up the Europol Convention.

72 *Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions* 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *OJ* L 135, 24.5.2016, p. 53–114.

73 See C. Blasi Casagran, "The new Europol Legal Framework: implications for EU exchanges of information in the field of law enforcement" in M.O'Neill and K Swinton (eds.), *Challenges and critiques of the EU internal security strategy* (Cambridge Scholars Publishing, 2017).

74 See, e.g., *Anniversary publication: 10 Years of Europol 1999-2009* (The Hague, Europol publications, 2009); V Mitsilegas, *EU Criminal Law* (Hart Publishing, 2009) 165.

75 A. Weyembergh, I. Armada and C. Brière, *The inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*, Study for the LIBE Committee, Brussels, 2014, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2014/510000/IPOL_STU%282014%29510000_EN.pdf, 24 ff.

addition to these databases, the Europol Platform for Experts provides specialists in a variety of law enforcement areas and private industry and academics with opportunities to discuss matters of interest to law enforcement, to share unclassified non-personal data to support investigative work and unclassified information and best practices on combating crime and to support training events.

The Member States have long remained reluctant to exchange information with each other and with Europol.[76] This could be explained by several factors. First, information at the national level tends to be compartmentalised at both the organisational and legal levels. It is often dispersed between several ministries, services and authorities, thus involving different degrees of secrecy. Coordination in the area of counterterrorism has proven particularly difficult.[77] Second, a lack of clear policy on information channels and on the protection of sensitive and confidential information has hampered effective cooperation with Europol for a long time.[78] Third, a concern arises from the fact that in Europol's work files the personal data of victims and witnesses are not separated from the personal data of criminals.

Data processed daily by Europol also come from other EU agencies (most importantly Eurojust and Frontex), EU information systems (such as VIS and SIS), private entities, third countries and public sources. A considerable proportion of these data are collected by national law enforcement authorities and in most cases are inserted automatically in the EIS. Article 7 of the 2016 Europol Regulation establishes the conditions under which the competent authorities in Member States must cooperate with Europol. The two interoperability proposals would facilitate law enforcement information-sharing between EU information systems and Europol databases. Access seems to be regarded as self-evident and few access requirements apply. National information systems and de-centralised EU information systems, instead, fall outside the scope of the two interoperability proposals. However, since national authorities feed the largest amount of information into Europol databases, the scope of the two proposals is *de facto* broader than what is formally envisaged.

3.4. The role of private actors: beyond the public/private divide

The information society has substantially changed the ways in which law enforcement authorities can obtain information and evidence. Beyond their own specialised databases, competent authorities have access to huge amounts of data in all types of public and private databases.

Nowadays the legal systems in most Western countries thus face relevant changes in the politics of information control. The rise of advanced technologies has magnified the capability of new players to control both the means of communication and data flows. To an increasing extent, public authorities are sharing their regulatory competences with an indefinite number of actors by imposing preventive duties on the private sector, such as information-gathering and sharing (e.g. on telecommunication companies

---

[76] International Centre for Migration Policy Development, *Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments*, JLS/2009/ISEC/PR/0001-F3, 9; E. Disley et al., *Evaluation of the implementation of the Europol Council Decision and of Europol's activities*, 2012, available at https://www.europol.europa.eu/sites/default/files/publications/rand_evaluation_report.pdf; O. Bures, "Europol's Counter-Terrorism Role: A Chicken-Egg Dilemma' in C Kaunert and S Léonard (eds.) *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe* (New York, Palgrave and Macmillan, 2013) 504. The issue emerged after the Madrid terrorist bombings, when Spanish police refused to share information on the types of explosives that had been used with their French counterparts.

[77] France, for example, has a centralised system, whereas Germany works at a more fragmented federal level. France has robust laws for detaining terrorist suspects and judges specifically trained to deal with the cases; other Member States do not.

[78] Council of the European Union, Third round of Mutual Evaluations, 'Exchange of information and intelligence between Europol and the Member States and among the Member States respectively,' Final Report, 13321/07, Brussels, 16 October 2007, at p 29.

for data retention purposes).[79] This trend is leading to a growing privatisation of surveillance practises. In this move, key players in private information society (producers, service providers, key consumers) are given law enforcement obligations.

Private actors are not just in charge of the operational enforcement of public authority decisions in security matters. They are often the only ones with the necessary expertise and therefore they profoundly shape decision-making and policy implementation. Their choices are nevertheless guided by reasons such as commercial interest and they are often unaccountable.

In the context of information sharing, and particularly in the area of interoperable information systems, technical platform integration (information hubs) functions across national boundaries and across the traditional public-private divide. Most of the web giants are established overseas, so that often private actors – voluntarily or compulsorily – transfer data to third countries. Companies do not just cooperate with public authorities but effectively and actively come to play a part in bulk collection and security practices. They identify, select, search and interpret suspicious elements by means of so-called 'data selectors.' Private actors, in this sense, have become 'security professionals' in their own right.

Systematic government access to private sector data is carried out not only directly via access to private sector databases and networks but also through the cooperation of third parties, such as financial institutions, mobile phone operators, communication providers and the companies that maintain the available databases or networks.

Personal data originally circulated in the EU for commercial purposes may be transferred by private intermediaries to public authorities, often also overseas, for other purposes, including detection, investigation and prosecution. The significant blurring of purposes among the different layers of data-gathering – for instance, commercial profiling techniques and security – aims to exploit the 'exchange value' of individuals' fragmented identities, as consumers, suspects of certain crimes, 'good citizens' or 'others.' Systematic government access to private-sector data may not only affect the exercise of civil and political liberties and the protection of fundamental rights, but also very intimate individual identity.

In this context, some have argued that the most important shortcoming of the 2016 data protection reform is that it resulted in the adoption of two different instruments, a Regulation and a Directive.[80] This separation is a step backwards regarding the objective envisaged by Article 16 TFEU – which instead promotes a cross-sectoral approach potentially leading to a comprehensive instrument embracing different policy areas (including the AFSJ) in the same way. This is a weakness because the level of protection envisaged by the 2016 Police Data Protection Directive is *de facto* lower than in the Regulation, as data gathering for law enforcement and national security purposes is mostly exempted from general data protection laws or constitutes an exemption under those provisions even at the EU level.[81] Furthermore, what happens in practice mostly depends on terms and conditions in contractual clauses signed by individuals every time they subscribe as clients of service providers and media companies.

---

79 V. Mitsilegas, 'The Transformation of Privacy in an Era of Pre-emptive Surveillance' (2015) 20 *Tilburg Law Review* 35-57; H E. De Busser, "Privatisation of information and the data protection reform" in S Gutwirth et al (eds.), *Reloading data protection: Multidisciplinary Insights and Contemporary Challenges* (Springer, 2013), pp. 129-149.

80 P. Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation" in M. Cremona (ed.), *New Technologies and EU Law* (OUP, 2017).

81 See Recital no. 19 and art. 2(d), GDPR.

Concluding remarks

During recent decades EU Member States have increased their efforts in the fight against terrorism, organised crime and illegal immigration, which have gradually developed a cross border dimension, accentuated by the dismantling of internal border controls. In the wider context of transnational cooperation, information exchanges are essential in fighting cross-border crime and to ensure a high level of security in the EU.

This working paper has explored how information management – and particularly interoperable information systems – is witnessing a paradigm change in the law-enforcement cooperation dynamics within the EU AFSJ.

Interoperability challenges existing modes of cooperation and integration in the EU AFSJ and also the existing distribution of competences between the EU and Member States, between law-enforcement authorities and intelligence services and between public and private actors, which are increasingly involved in information-management activities. Crucial in this process is, first, a new form of platform integration which partially sidelines harmonisation, and also the principle of availability, which complements and redefines the boundaries of mutual recognition. Second, large-scale information exchanges via interoperable information systems have progressively eroded the boundaries between law enforcement and intelligence services. Moreover, they have facilitated a reshuffling of responsibilities and tasks within the law enforcement community, for instance between security and migration actors. This process has gone hand in hand with an increase in the number and powers of EU agencies in the AFSJ. Furthermore, competent authorities have access to huge amounts of data in all types of public and private databases. Interoperable information systems function not only across national boundaries but also across the traditional public-private divide.

The issues explored in the course of this paper indicate further questions that need to be addressed. There is a need to study whether and how the information gathered and/or accessed by law enforcement and judicial authorities via interoperable information systems may be used not only as clues during an investigation but also as evidence at trial. [82] Future research must therefore turn to existing models in national law that can serve as either examples or counter-examples of the use of (e.g. intelligence) information in trials. Over the years, several authors have discussed whether and how to envisage the 'judicialization of information.'[83] There are, of course, a number of procedural and evidentiary issues to address, possibly reimagining procedural traditions, regarding the possible admissibility criteria for improperly obtained evidence. The possibility of using information in trials can also indirectly regulate gathering and processing means and safeguards in order for information to meet admissibility requirements. Certain Member states, including Italy, establish clear limits on the admissibility/employability of evidence in trials, depending on how the information has been gathered and stored.[84]

In the end, where it is construed in such a way that is compatible with the protection of individual rights, law enforcement access to interoperable databases with a view to prosecuting serious crime (including terrorism) can be a precious source of information and therefore a desirable alternative to the introduction of administrative measures or the distortion of criminal justice principles with an endless criminalisation of preparatory offences in the realm of terrorism. Nevertheless, with reference to interoperable information systems, the question is whether models grounded on admissibility

---

[82] See D. Bigo et al, *National Security and secret evidence in legislation and before the courts: exploring the challenges*, Study for the LIBE Committee, European Parliament, PE.509.991 (Brussels, 2014).

[83] See e.g. K.L. Scheppele, "The Ground-Zero Theory of Evidence" (1998) 49(2) Hastings L.J. 321, at https://repository.uchastings.edu/hastings_law_journal/vol49/iss2/3; K.L. Scheppele, "The deep dilemma of evidence in the global anti-terror campaign" in F. Fabbrini and V.C. Jackson, *Consitutionalism across borders in the struggle against terrorism* (Edward Elgar, 2016), Ch 8.

[84] art. 191 *c.p.p.* – "Prove illegittimamente acquisite." Italian Code of Criminal Procedure on Evidence inadmissibility.

requirements can be applied to speculative security practices.[85] The current bulk collection of data implies, in fact, that information is gathered and stored for no specific purpose and therefore it is more difficult to attach a specific procedure including mandatory legal guarantees regarding its use.

[85] In the context of speculative security, individuals are targets of public authority measures; information is gathered irrespective of whether and how it could be used to charge the suspect of a criminal offence or use it in criminal proceedings and eventually at trial. Law enforcement authorities can thus act not only in the absence of harm, but even in the absence of suspicion. See M. De Goede, *Speculative security* (University of Minnesota Press, 2012).

Author contacts:

Francesca Galli

Jean Monnet Fellow 2017/18

Robert Schuman Centre for Advanced Studies, European University Institute

Villa Schifanoia, Via Boccaccio 121

I-50133 Florence

Email: Francesca.Galli@eui.eu