UNIO - *EU Law Journal*. Vol. 5, No. 2, July 2019, pp 128-135.

School of Law – University of Minho

Recent developments of interoperability in the EU Area of Freedom, Security and Justice: Regulations (EU) 2019/817 and 2019/818

Alexandre Au-Yong Oliveira*

ABSTRACT: Regulation 2019/817 and Regulation 2019/818 establish a framework for the interoperability between EU large scale information systems in the Area of Freedom, Security, and Justice. The new rules on interoperability aim at providing easier information sharing and to improve security in the EU, while safeguarding fundamental rights. This presupposes that the data is fully trustworthy and only accessed in legitimate ways. Due to the nature of the data, especially biometric data, and the scale of the databases, security is an obvious concern. These problems imply a high level of trust between the Member States, persons and entities that will use the information systems. Trust between Member States is not an axiom in the present context of the EU as recent CJEU decisions reveal and imply, among other aspects, a common institutional background.

KEYWORDS: Schengen Area – interoperability – cooperation – mutual trust – privacy.

* Portuguese judge and lecturer at the Portuguese Centre for Judicial Studies (Centro de Estudos Judiciários - CEJ).

1. Introduction

This paper shall be presented from the point of view of a EU judicial operator as the Author is a judge of a Member State (Portugal) and presently a lecturer at the Portuguese Centre for Judicial Studies (hereinafter, "CEJ"), the school that aims at preparing its students for the functions of national public prosecutor and judge. The Author lectures both Criminal Law and International Judicial Cooperation in Criminal Matters at CEJ.

Interoperability is quite a new concept for judicial operators, but it is a very interesting concept especially for the field of international police and judicial cooperation in criminal matters. After all, police and judicial cooperation presuppose two or more different legal systems working with one another, for example by exchanging information (*e.g.*, identity data), gathering evidence (*e.g.*, oral statements, documents, DNA samples, digital data, etc) or arresting a person, in a different country where the procedure, investigation or trial is ongoing.[1]

International cooperation in general is increasingly important today due to substantial increases in world mobility[2] and interconnectivity.[3] That need is even greater in the European Union where internal national borders practically do not exist. As Article 3(2) of the Treaty on European Union (hereinafter, TEU) states: *"The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime".*

[1] Interoperability may be defined as a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, at present or in the future, in either implementation or access, without any restrictions. While the term was initially defined for information technology or systems engineering services to allow for information exchange, a broader definition takes into account social, political, and organizational factors that impact system to system performance. The concept of interoperability differs from neighbouring concepts like **integration**, **compatibilization** or **portability**. Integration happens when two or more functions or components of the same system interact. Compatibility when two or more applications work in the same environment. Portability happens when an application can be transported from one environment to a different one without losing capabilities.

[2] Human circulation today is increasingly intense, be it through migration or simply through tourism. According to a UN 2017 report on migration, *"The number of international migrants worldwide has continued to grow rapidly in recent years, reaching 258 million in 2017, up from 220 million in 2010 and 173 million in 2000. Over 60 per cent of all international migrants live in Asia (80 million) or Europe (78 million). Northern America hosted the third largest number of international migrants (58 million), followed by Africa (25 million), Latin America and the Caribbean (10 million) and Oceania (8 million).". Albeit this significant inflow of migrants to Europe, it should be noted that "In Europe, instead of growing by two per cent, the size of the population would have fallen by one per cent in the absence of a net inflow of migrants."*. Following the same report the main destinations of migration in Europe were **Germany** - around 12 million -, and the **UK** – nearly 9 million (*in* https://www.un.org/en/development/desa/population/migration/publications/migrationreport/docs/MigrationReport2017_Highlights.pdf). Where tourism is concerned Europe received 713 million tourists in 2018 while in 2000 it hosted 391 million tourists (*in* https://ourworldindata.org/tourism).

[3] Cyberspace substantiated today in the Internet and the Wide World Web, as we all know, implies the deterritorialization of many human activities including criminal activities. On recent trends in cyber-dependent crime (crimes that may only be committed through information systems, for example ransomware infection) and cyber-related crime (crimes that are not unique to or require information systems, for example the distribution of child pornography) see Europol's European Cybercrime Centre (EC3) yearly reports *in* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment.

To compensate for this absence of internal (mutual) borders in the Schengen Area,[4] the Schengen provisions abolish checks at the Union's internal borders, while tightening controls at the external borders, in accordance with a single set of rules. These rules cover several areas such as the existence of a common set of rules applying to people crossing the EU external borders, including types of visa needed, conditions of entry and how checks at external borders should be carried out; enhanced police cooperation (including rights of cross-border surveillance and hot pursuit); stronger judicial cooperation through a faster extradition system and transfer of enforcement of criminal judgments.[5] Also related to these problems, the EU foresees common policies on international protection (including asylum) and immigration.[6]

As we will see, to improve the application of these common rules and policies, in recent years the EU has legally foreseen multiple information systems to be technically implemented in the near future on top of updating the already existing information systems.[7] In addition, the EU has very recently adopted a legal basis to make all these systems interoperable between themselves.

The present paper will focus on these recent developments of interoperability in the EU of particular relevance in the Area of Freedom, Security and Justice, specifically Regulation 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 (hereinafter, "Regulation 2019/817) and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (EU) and Regulation 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (hereinafter "Regulation 2019/818").

2. Interoperability: Regulations 2019/817 and 2019/818

On 14 May 2019, the Council adopted two regulations, Regulation 2019/817 and Regulation 2019/818, establishing a framework for the interoperability between EU large scale information systems (databases) in the Area of Freedom, Security, and

[4] The Schengen Area has its origins in 1985 *"when cooperation between individual governments led to the signing, in Schengen (a small village in Luxembourg), of the Agreement on the gradual abolition of checks at common borders, followed by the signing in 1990 of the Convention implementing that Agreement. The implementation of the Schengen Agreements started in 1995, initially involving seven EU States. Born as an intergovernmental initiative, the developments brought about by the Schengen Agreements have now been incorporated into the body of rules governing the EU. Today, the Schengen Area encompasses most EU States, except for Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom. However, Bulgaria and Romania are currently in the process of joining the Schengen Area. Of non-EU States, Iceland, Norway, Switzerland and Liechtenstein have joined the Schengen Area."* (*in* https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en).

[5] See article 77(2) of TFEU and the Schengen *acquis* as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999 (in https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2000:239:FULL&from=EN).

[6] Articles 78 and 79 of TFEU

[7] We use "information system" as meaning *"a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance"* (article 2(a) of Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA).

Justice. The new rules on interoperability, upon which the European Parliament agreed in April 2019, aim at providing easier information sharing and to "*considerably improve security in the EU, allow for more efficient checks at external borders, improve detection of multiple identities and help prevent and combat illegal migration[, terrorism and other serious crimes]. All this while safeguarding fundamental rights*".[8]

The two regulations are closely related and should be read together. It should be noted that the information systems and their foreseen interoperability, essentially aiming at the improved control of external borders, will mainly affect third-country nationals.

The adoption of two regulations instead of one result from the need to respect the distinction between systems that concern:

a) the Schengen acquis regarding borders and visas (i.e. the VIS, the EES, the ETIAS and the SIS as regulated by Regulation (EC) nº 1987/2006),

b) the Schengen acquis on police cooperation or that are not related to the Schengen acquis (the Eurodac system, the European Criminal Records Information System for third-country nationals and the Schengen Information System as regulated by Council Decision 2007/533/JHA).

The Regulations pursue the aim of establishing interoperability between the following databases:

i. Three existing EU information systems:

a) The **Schengen Information System** (hereinafter, "SIS"), that contains alerts about wanted or missing people and objects[9].

b) The **Eurodac** system that contains the identity, including fingerprints, of asylum applicants who have been registered in EU Member States and associated countries. This database serves the implementation of the Dublin regulation that determines which EU Member State (hereinafter, "MS") is responsible for the examination of an application for asylum. It helps to: a) verify whether an applicant has previously claimed asylum in another Member State; b) check whether an applicant has previously been apprehended when entering European territory unlawfully; c) determine which Member State is responsible for examining an asylum application.[10]

c) The **Visa Information System** (hereinafter "VIS"), that is used to register and check persons applying for a visa to enter the Schengen area. Authorities can use the VIS to perform biometric matching to identify people and prevent identity theft or fraud.[11]

ii. Three EU information systems that are still in an implementation phase:

a) the **Entry/Exit System** (hereinafter, "EES"), that will register entry, exit and refusal of entry information of non-EU nationals crossing the external borders of the Schengen area.[12]

[8] https://www.consilium.europa.eu/en/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/.

[9] In the near future the SIS will be updated to include other kinds of alerts and to expand its data types, including facial images and DNA profiles. For an overview consult https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/schengen-information-system-council-adopts-new-rules-to-strengthen-security-in-the-eu/. For the legal basis see Regulations (EU) 2018/1860, (EU) 2018/1861 and (EU) 2018/1862.

[10] Regulation (EU) Nº 603/2013.

[11] Regulation (EC) Nº 767/2008.

[12] Regulation (EU) 2017/2226.

b) the **European Travel Information and Authorisation System** (hereinafter, "ETIAS"), which allows and keeps track of visitors from countries who do not need a visa to enter the Schengen Zone.[13]

c) the **European Criminal Records Information System for third-country nationals** (hereinafter "ECRIS-TCN");[14]

iii. the **Interpol's** Stolen and Lost Travel Documents (hereinafter "SLTD") database;

iv. parts of **Europol's** database.[15]

The interoperability between these (eight) systems will consist of four components:

a) A **European search portal** (hereinafter "ESP") to search simultaneously in all the EU information Europol and Interpol systems. As the regulations state in their Recitals: *"the ESP should act as a single window or 'message broker' to search the various central systems and retrieve the necessary information seamlessly and in full respect of the access control and data protection requirements of the underlying systems"* (Recital 13).

b) A **shared biometric matching service** (hereinafter "BMS") to search and cross-check biometric data in the EU information systems. As the regulations state: *"the main purpose of the shared BMS should be to facilitate the identification of an individual who is registered in several databases, by using a single technological component to match that individual's biometric data across different systems, instead of several components. (…) The shared BMS should regroup and store all these biometric templates – logically separated according to the information system from which the data originated – in one single location, thereby facilitating cross-system comparisons using biometric templates and enabling economies of scale in developing and maintaining the EU central systems"* (recital 18).

c) A **common identity repository** (hereinafter "CIR") containing biographical and biometric data of non-EU citizens available in several EU information systems. *"The CIR should provide for a shared container for identity data, travel document data and biometric data of persons registered in the EES, VIS, ETIAS, Eurodac and the ECRIS-TCN. It should be part of the technical architecture of these systems and serve as the shared component between them for storing and querying the identity data, travel document data and biometric data they process"* (Recital 25).

d) A **multiple identity detector** (hereinafter "MID") to detect multiple identities linked to the same set of biometric data. *"The MID should create and store links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for bona fide travellers and combating identity fraud. The MID should only contain links between data on individuals present in more than one EU information system. The linked data should be strictly limited to the data necessary to verify that a person is recorded in a justified or unjustified manner under different identities in different systems, or to clarify that two persons having similar identity data may not be the same person"* (Recital 39).

As we can easily infer from these brief descriptions, when the information systems become fully interoperable, they will be a very powerful technical tool for the referred to purposes[16]. The technical aspects of all these systems and interoperability

[13] Regulation (EU) 2018/1240.

[14] Regulation (EU) 2019/816.

[15] Including data on people suspect of having committed crimes or for whom there is reasonable grounds to believe they will commit a criminal offense (see article 18(2)(a), (b) and (c) of Regulation (EU) 2016/794 and articles 4(16) of Regulations (EU) 2019/817 and 2019/818).

[16] The concrete date for the interoperability is not stated in the regulations and depends on technical factors mainly of the responsibility of eu-LISA.

components are to be managed by a sole entity, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (hereinafter "eu-LISA").[17]

3. Some common problems

When we speak of the improved detection of multiple identities and the prevention and combat of illegal migration, terrorism and other serious crimes, we presuppose that the available data is trustworthy, that it fully corresponds to reality. Obviously all systems, be them in digital form or in other mediums (for example, paper archives) bring with them risks of error caused by mere accident or by an intentional behaviour on the part of certain types of persons. Sometimes it is difficult to correct these mistakes or at least it takes time. As a criminal judge, the author has encountered mistakes made by court clerks while inserting names, ages, addresses, types of crimes committed, etc., in criminal records. The author also encountered multiple identities of convicted people in criminal records, including ones that are only detected or corrected years after their inclusion in the official records.[18] These risks are further enhanced by the large-scale information systems here concerned (in part used to detect multiple identities), that evidently imply a very high level of mutual trust between MS, national authorities and agencies involved in the inputting, updating and accessing of data.

On the other hand when we talk about safeguarding fundamental rights, considering that the interoperability components, especially the shared BMS automatically processing and granting access to sensitive personal data[19] such as fingerprint data or facial images, that is connected to biographical data (name, nationality, residence, etc) and other important data like criminal records, we have to take into account, in particular, the fundamental rights foreseen in Articles 7 and 8 of the Charter of Fundamental Rights of the EU (CFREU), the right of respect for private and family life and the right to protection of personal data.

Due to the nature of the data, especially biometric data, and the aimed interoperability of these large scale databases, as the Cambridge Analytica scandal and today's ever more frequent data breaches teach us (with the subsequent illegal use or acquisition of data), internal and external security is obviously of the utmost importance. Cyberattacks, for example in the form of distributed denial of services (DDOS) or ransomware, are also very real and big problems in this domain.

The Regulations try to address these problems in technical terms, for example, by foreseeing specific profiles of the people that may access the systems, by explicitly

[17] For an overview of eu-LISA consult https://www.eulisa.europa.eu/About-Us/Who-We-Are.

[18] For example, it is not unusual for courts to convict a certain person as the author of various criminal offences judged in different and separate casefiles to only later, for example, while executing a custodial sentence, discover that in each of them he was using a different identity based on forged documents. These identities sometimes include, apart from different names and parents, different nationalities.

[19] 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (article 4(1) of Regulation (EU) 2016/679 (GDPR)); 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (article 4(14) of Regulation (EU) 2016/679 (GDPR)).

keeping logs of accesses, by tightening transfers of data to third parties and conceding specific rights to the data subjects like the right of access, rectification and erasure of personal data stored in the MID. All of this while foreseeing important supervisory powers by independent entities including the European Data Protection Supervisor (hereinafter "EDPS").

But, as the EDPS pointed out before the final versions of the regulations were approved: *"Interoperability is not primarily a technical choice, it is in particular a political choice to be made. Against the backdrop of the clear trend to mix distinct EU law and policy objectives (i.e. border checks, asylum and immigration, police cooperation and now also judicial cooperation in criminal matters) as well as granting law enforcement routine access to non-law enforcement databases, the decision of the EU legislator to make large-scale IT systems interoperable [will] not only permanently and profoundly affect their structure and their way of operating, but [will] also change the way legal principles have been interpreted in this area so far and [will] as such mark a 'point of no return'".*[20]

In addition to all this and where judicial cooperation in criminal matters is concerned, it should be noted that the latest developments in the CJEU case-law are not very indicative, to say the least, of a general environment of mutual trust between MS.

For example, through a judgement issued on the 27 of May 2019, in joint cases C-508/18 and C-82/19 PPU, concerning a preliminary ruling requested by the Supreme Court of Ireland, the CJEU ruled that public prosecutors offices of a MS, in the concrete case Germany's, cannot be considered "judicial authorities" for the effect of issuing an European Arrest Warrant, if they: *"are exposed to the risk of being subject, directly or indirectly, to directions or instructions in a specific case from the executive, such as a Minister for Justice, in connection with the adoption of a decision to issue a European arrest warrant".*

Furthermore, through a judgement issued on the 25 of July 2019, in case C-216/18, concerning a preliminary ruling requested by the High Court of Ireland, the CJEU ruled that where the executing judicial authority, called upon to decide whether a person in respect of whom a European arrest warrant has been issued for the purposes of conducting a criminal prosecution, is to be surrendered, has material indicating that there is a real risk of breach of the fundamental right to a fair trial on account of systemic or generalised deficiencies concerning the independence of the issuing Member State's judiciary. In the concrete case Poland, that authority must determine, specifically and precisely, whether there are substantial grounds for believing that that person will run such a risk if he is surrendered to that State.

This last decision involving Poland's institutions has, as a backdrop, introduced recent changes to the constitutional role of the National Council for the Judiciary in safeguarding independence of the judiciary, in combination with the Polish Government's invalid appointments to the Trybunal Konstytucyjny (Constitutional Tribunal) and its refusal to publish certain judgments, and other legislative initiatives that clearly affect the independence of the polish judiciary, like the compulsory retirement of some of their Supreme Court judges. These legislative measures with the clear weakening of the sacred (European) principle of separation of powers, thus affecting the essence of the fundamental right to a fair trial, were all critically analysed in the Commission's reasoned proposal of 20 December 2017, submitted for a Council Decision on the determination of a clear risk of a serious breach by the Republic of Poland of the rule of law, in accordance with Article 7(1) of the TEU.

[20] GDPS, *in* Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems.

What these recent cases reflect, in the author's opinion, is that the principle of mutual recognition and the underlying mutual trust that are supposed to be the cornerstones of the system of judicial cooperation in criminal matters between MS[21] are not to be taken for granted and are, at the moment, far from being axioms that every MS can blindly accept.[22] What these cases illustrate is that mutual trust is not something that derives from a mere nominal categorization acquired by becoming a MS, but presupposes national institutional backgrounds that in some cases, even in the EU, are still quite distant from each other and/or that can quickly change and ground legitimate suspicions on key democratic values like judicial independence.

So if we transpose these problematizing ideas to the interoperability here in question, that, as mentioned, presupposes a high level of mutual trust between MS, we may find even more difficulties than those present in judicial cooperation in criminal matters, for the input and access to those interoperable information systems will be done mainly through governmental agencies like Ministries of Foreign Affairs where visas and asylum requests are concerned, or by law enforcement agents for the prevention and/or investigation of illegal immigration and serious criminal offences.

Obviously, the author is not questioning the need for this interoperability in today's digital day and age, but, as the EDPS and other authors have pointed out,[23] the interoperability in question, involving so many states and agencies and large-scale databases, is not merely a technical decision but also a political one, with many (political and juridical) implications for the near future.

[21] The principle of mutual recognition is now stated in article 67(3) of the TEU and article 82 of the TFEU. It was at Tampere (Italy) that the European Council - the EU summit of the leaders of its 15 member states - met in a special session in October 1999 to give a kick-start to the EU's justice and home affairs (JHA) policies, establishing mutual recognition, based on mutual trust, as the cornerstone of EU judicial cooperation in criminal matters.

[22] As was stated not too long ago by the CJEU, "the principle of mutual trust between the Member States is of fundamental importance in EU law, given that it allows an area without internal borders to be created and maintained. That principle requires, particularly with regard to the area of freedom, security and justice, each of those States, save in exceptional circumstances, to consider all the other Member States to be complying with EU law and particularly with the fundamental rights recognised by EU law" (*in* Opinion 2/13 of the Court, of 18 December 2014, paragraph 191, *in* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CV0002).

[23] For concrete examples of problems that arise in terms of the trustworthiness of the information systems in question see Evelien Brouwer, "Interoperability of Databases and Interstate Trust: a Perilous Combination for Fundamental Rights" (*in* https://verfassungsblog.de/interoperability-of-databases-and-interstate-trust-a-perilous-combination-for-fundamental-rights/).