ORIGINAL SCIENTIFIC PAPER

UDK: 351.74
Received: November 2021

DUNJA DUIĆ*, MARIJO ROŠIĆ**

Interoperability between the EU information systems – from an idea to the realisation

Summary

This article provides an overview of the emergence of the interoperability of the EU system, the main goal of which is to interconnect six EU databases into a single system that will improve the general security situation of the EU and combat illegal migration. TThe first part of the article detailedly describes the legal framework that preceded the establishment of the interoperability of EU information systems and explains the reasons for its establishment. The article describes the purpose of each individual system and their interdependence, interconnectedness and practical operation. Based on this interdependence, the article further describes some scenarios of practical application and possible implications for the work of law enforcement and other agencies in the EU. The authors explain the similarities of PNR system application and interoperability. By analysing the available case law in the application of PNR, the authors analyse the possible judicial consequences of the application of the principle of proportionality in the future practical implementation of interoperability. Additionally, through analyses of future scenarios of practical implementation of interoperability, the article points out possible implementation and legislative shortcomings. The article is based on a comparative, historical method and case analysis.

Keywords: *Interoperability, proportionality, PNR, SIS, EU VIS, EES, ETIAS, Eurodac, ECRIS-TCN.*

---

* Dunja Duić, PhD, LLM (Ghent), Associate Professor dduic@pravos.hr Josip Juraj Strossmayer University of Osijek,Faculty of Law.

** Marijo Rošić, M.A. in Law, M.A. in Criminalistics, Liaison Bureau Croatia in Europol- Head, Ministry of Interior.

This paper is a product of work that has been fully supported by the Faculty of Law Osijek Josip Juraj Strossmayer, University of Osijek, under the project nr. IP-PRAVOS-6 „implementation of EU Law in Croatian Legal System".

1. INTRODUCTION

The terrorist attack in Madrid in 2004 in which 194 people were killed, the suicide bombings in London in 2005, the bloody terrorist attack on the redaction of the satiric journal Charlie Hebdo in January 2015 in Paris, the series of terrorist attacks in Paris organized on November 13 2015 during which more than 130 people were killed, the attack on the Christmas Fair in Berlin in 2016 with 12 casualties and 55 injured and a number of other terrorist activities that have taken place have led to a stronger reflection on how to prevent future attacks. At the same time, at the end of 2015, the EU was facing perhaps the biggest challenge in its history: how to control the arrival of an enormous number of illegal migrants who began to enter the EU uncontrollably. It was necessary to respond to the deterioration of the EU's internal security by introducing an additional package of measures to strengthen the security and repressive apparatus (immigration, border guards and law enforcement), but also the judicial system (raising awareness on the new modus operandi of criminal activities among the judicial authorities). Further activities were directed to strengthening capacity at external borders, strengthening data collection within different systems, processing data on migrants and introducing tools to prevent terrorism, organized crime and illegal migration. A prerequisite for further work was the strengthening of the information exchange and the introduction of information management including an interoperable solution. It has been found that most of the systems used by law enforcement and other agencies are not interoperable.

What does it mean that the systems are not interoperable? Even before these efforts, there were EU systems that were centralized and used in a standardized way. These systems also showed shortcomings and were not "networked" enough to meet the real challenge: to exchange data and share all needed information. In addition to the existing ones, it was necessary to plan the establishment of a solution that will prevent the existence of current „blind spots". The introduction of biometrics with the interoperability package sought to unequivocally remove all the possible obstacles to establish the identity of persons. In parallel with these processes, the EU is strengthening fundamental rights, especially protection of personal data. As huge amounts of (personal) data will be processed through all existing and future systems, it is necessary to ensure adequate control over the processing of (personal) data in accordance with the highest security and data protection standards.

This article starts from following research questions: What does the Interoperability of the EU systems mean? Is the principle of proportionality adequately implemented in relation to personal data protection? The article clarifies the similarities between PNR and interoperability. By analysing the case law related to the practical application of PNR, the authors analyse the application of the principle of proportionality to the processing of a large set of data that could be applicable in the implementation of interoperability. This article, in addition to the questions asked, also refers to possible *de lege ferenda* legal solutions that could improve the application of interoperability based on the realistic scenarios of its future implementation.

2. THE AREA OF FREEDOM, SECURITY AND JUSTICE – FROM THE PRINCIPLES OF COMMON COOPERATION TO THE INTEROPERABILITY BETWEEN THE EU INFORMATION SYSTEMS

The Area of Freedom, Security and Justice (hereinafter: AFSJ) is today regulated in Chapter V of the Treaty on the Functioning of the EU (hereinafter: TFEU), in Articles from 67 to 89 of the TFEU. The focus of this paper is police cooperation, Schengen and cooperation in criminal matters. However, in order to understand today's regulation of the AFSJ, it is necessary to look at the development of this EU policy.

The EU's institutional framework that precedes AFSJ law has gone through several phases of development. Before the entry into force of the Maastricht Treaty cooperation was purely informal and intergovernmental. The Maastricht Treaty created a hybrid system that has been accepted in the literature as the "Three Pillars" that make up the EU. The first pillar included the powers of the European Community (the European Economic Community hereby changes its name to the European Community (hereinafter: the EC)), the second the Common Foreign and Security Policy (hereinafter: CFSP (Chapter V)), and the third Justice and Home Affairs (hereinafter: JHA (Chapter VI)). It should be emphasized at this point that for the purposes of this paper, the approach based on the so called "Three Pillars" analysis will be used as a standard, although there are many authors who relativize or challenge the division of EU law into "Three Pillars".[1] Such a hybrid system already at the time of its creation indicated a number of possible problems and unresolved situations. For example, Member States have decided that the decision-making system of the first pillar does not apply to the second and third pillars. It was decided that the second and third pillars would be an area of intergovernmental cooperation, which on the one hand allowed the monopolization of the decision-making process by the Council of Ministers. The rules for JHA area "third pillar "provided that the Council is authorized to make decisions unanimously, there was very limited role of European Commission (hereinafter: COMM) and the Court of Justice was not awarded any mandatory jurisdiction which is completely different from policies defined in Community law.[2] JHA area covered asylum policy, rules governing the crossing of the Union's external borders, immigration policy and policy regarding third-country nationals, combating drug addiction and fraud on an international scale, judicial cooperation in civil and criminal matters and customs and police cooperation.

One of the important aspects of JHA is Schengen area. The free movement of goods, persons, services and capital was the founding principle of EU integration. For that reason, Schengen area and cooperation were founded by the Schengen Agreement[3] that was signed

---

[1] Wessel, R. (2000). *The Inside Looking Out: Consistency and Delimitation in EU External Relations*. Common Market Law Review, 37/5, 1135-1171; Bogdandy Von, A., Nettesheim, M. (1996). *Ex Pluribus Unum: Fusion of the European Communities into the European Union*. European Law Journal, Nr. 2/3, 267-289; Heukels, T; Blokker, N.; Brus, M. (ur), (1998). *The European Union after Amsterdam — A Legal Analysis.* Kluwer; The Hague. 51 – 68.

[2] Muller-Graff, P. (1994). *The legal bases of the third pillar and its position in the framework of the Union. Treaty*'.Common Market Law Review, 493; Cuirtin, D. (1993). *The constitutional structure of the Union: a Europe of bits and pieces*. Common Market Law Review, 17.

[3] The full name of the Agreement is: Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders; Official Journal L 239 , 22/09/2000. p. 13 – 18.

on 14 June 1985 by five of the ten EU Member States in the town of Schengen (Luxembourg). Due to the lack of consensus amongst European Economic Community Member states, the Schengen Area was established outside of the then European Economic Community.[4] The Agreement proposed the abolition of border checks at the common borders and it established short-term measures simplifying internal border checks and coordination of the fight against drug trafficking and crime.[5] In 1990, the Agreement was supplemented by the Schengen Convention that was signed on 19 June 1990.[6] The Convention, which took effect in 1995, sets out how the abolition of internal border control (Art. 2.1.) should be implemented, as well as a series of necessary accompanying measures: external border control (Art. 3–8); harmonization of visa legislation (Art. 9–27); asylum procedures (Art. 28–38); police cooperation and security measures (Art. 39–91). Furthermore, the Schengen Convention introduced a joint information system: the Schengen Information System (hereinafter: SIS), which is designed to help maintaining public order and security and it allows national border control and judicial authorities to obtain information on persons or objects. (Art. 92–119). The SIS can be regarded as the "cornerstone" of Schengen.[7] Conclusively, the Schengen Convention aimed at the abolition of internal borders, the strengthening of external border checks, as well as defining procedures for the issuing of uniform visas and measures.[8]

Free circulation of people as provided for by the Schengen Agreement and Schengen Convention was implemented on 26 March 1995, all European Union Member States except the United Kingdom and Ireland signed the Schengen Agreement.[9] This means that thirteen (of a then total of fifteen) Member States of the EU created a legal area technically outside of the Union/Community legal order, *inter alia* with the free movement of persons and

---

[4] Schutte, Julian J. E. (1991). *Schengen: it's meaning for the free movement of person in Europe*. Common Market Law Review 28, 550.

[5] Nanz, K.P. (1995). *The Schengen Agreement: Preparing the Free Movement of Persons in the European Union*. in Bieber, R./Monar, J. (eds.1995). *Justice and Home Affairs in the European Union. The Development of the Third Pillar*, Brussels, 29-48.

[6] The full name of the Convention is: Convention implementing the Schengen Agreement of 15 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the gradual abolition of checks at their common borders.

[7] Baldwin-Edwards, M./Haberton, B., (1994). *Will SIS be Europe's Big Brother*, in Anderson, M./Den Boier, M. (eds.). (1994). Policing Across National Boundaries, London/New York: Pintzer. (1994), 133-157.

[8] See more in literature on the Schengen Convention: Schutte, J.J.E. (1991). *Schengen: Its Meaning for the Free Movement of Persons in Europe*. Common Market Law Review, 549–570; Meijer, H., Bolten, J.et al. (eds) Schengen. Internationalisation of Central Chapters of the Law of Aliens, Refugees, Privacy, Security, and the Police (Antwerp: Kluwer), pp. 5-6; Curtin, D., Meijers, H., (1995). *The Principles of Open Government in Schengen and the European Union: Democratic Retrogression?* 32 Common Market Law Review, 391–441; O'Keeffe, D. (1991). *The Schengen Convention: A Suitable Model for European Integration?* Yearbook of European Law, 185–219; Schutte, J.J.E. (1993). *The European Market of 1993*. Criminal Law Forum, 55–83; Woltjer, A., (1995). *Schengen: The Way of No Return?* Maastricht Journal, 256-278;
Hailbronner, K., Thierry, C. (1997). *Schengen II and Dublin, Responsibility for Asylum Applications in Europe*. Common Market Law Review, 957-989.

[9] The Accession Protocols and Agreements to the 1985 Agreement and the 1990 Implementation Convention with Italy (signed in Paris on 27 November 1990), Spain and Portugal (signed in Bonn on 25 June 1991), Greece (signed in Madrid on 6 November 1992), Austria (signed in Brussels on 28 April 1995) and Denmark, Finland and Sweden (signed in Luxembourg on 19 December 1996), with related Final Acts and declarations; see more about this stage of Schengen integration in: *Schengen: The pros and cons: Editorial comment*, (1995) . Common Market Law Review 32, 673-678.

police cooperation.[10] The Schengen Convention, which set out how the abolition of internal border control would be applied, was signed just after the fall of the Berlin Wall in 1989 and just before the creation of the European Union by way of the Maastricht Treaty in 1992. The Maastricht Treaty and a new pillar system that institutionalized cooperation in the field of justice and home affairs within the framework of the Third Pillar of the Union[11] created necessary legal ground for incorporation of the Schengen acquis into the Union's legal and institutional framework which happened in Amsterdam Treaty.

The formal incorporation of the Schengen acquis into the Amsterdam Treaty was achieved by way of Protocol (No 2) as annexed to the Treaty.[12] Protocol (No. 2) incorporates the developments brought about by the Schengen Agreement into the EU framework. The Schengen acquis is form then entirely within the legal and institutional framework of the EU. In order to integrate the Schengen acquis into the EU legal framework, two compromises were made in the Schengen Protocol. Firstly, Article 1 of the Protocol empowered closer cooperation between the Schengen Agreement signatories. In this way, the UK, Ireland and Denmark were able to stay outside.[13]

The Treaty of Amsterdam (hereinafter: TEC) not only incorporated the Schengen acquis into the European legal framework, but it also provided the Community with the powers for the regulation of external borders, by transferring visa, asylum, immigration and other policies pertaining to free movement of persons from the Third Pillar to Title IV TEC[14]. What remained in the Third Pillar was the police and judicial cooperation in criminal matters.[15] This produced a double decision regime for the Schengen acquis (Community method for the TEC-regulated policies and intergovernmental method for the Treaty on the European Union (hereinafter: TEU) policies). It is important to mention that the transfer of justice and home affairs powers to the Treaty establishing the European Community (TEC) involved a five-year transitional period in which the Commission shared its right of initiative with the Member States. The said period ended on 1 May 2004. During the transitional period, the decision-making process within the Council required a unanimous vote, with a right of consultation for the Parliament, and the Court of Justice had restricted jurisdiction (references for a preliminary ruling from final courts only).[16]

The Treaty of Nice already entered into force when the transitional period for the First Pillar provisions was over (1 May 2004). In fact, the Nice Treaty made some modest changes to these provisions[17]: the number of areas became subject to the co-decision procedure,

---

[10] Article 134 Schengen convention "http://www.hri.org/docs/Schengen90/body8.html" - accessed 16 October 2021.

[11] Third pillar was named: Justice and Home Affairs (JHA).

[12] Protocol (No 2) integrating the Schengen acquis into the framework of the European Union (OJ 1997 C 340, at 93).Amsterdam Treaty (http://www.europarl.europa.eu/topics/treaty/pdf/amst-en.pdf - accessed 29 September 2021).

[13] Ibidem, Article 1.See more: Wagner 1998, p. 1-60: Leidenmuhler 2002, p. 253-275.

[14] Article 61-69 TEC - Amsterdam.

[15] Title VI TEU-Amsterdam (Art. 29–42 TEU) was renamed from Justice and home affairs to the Police and judicial cooperation in criminal matters. Amsterdam Treaty, English version available at: http://www.lexnet.dk/law/subjects/treaties.htm.

[16] Art. 68.1 TEC. See more in literature: Rijpma 2009, p. 94.

[17] Art. 67.5 TEC-Nice and a new Protocol concerning Art. 66 TEC-Nice; English version available at: http://www.lexnet.dk/law/download/treaties/Ect-2001.pdf - accessed 25 September, 2021

although several areas remained subject to unanimity of the Council with consultation of the European Parliament (family law, migration).[18] Also, the Court of Justice's jurisdiction in the area was still limited, despite the fact that there were efforts of the Commission to expand it.[19] The most important change in the Third Pillar provision was the introduction of a Framework Decision (these legal acts resembled Directives, but according to the Court of Justice decisions, they had no direct effect).[20]

Continuous disputes about the boundaries between the Third Pillar and the EC Treaty rules were resolved with the Lisbon Treaty.[21] The Lisbon Treaty resolved this issue with the abolition of the Third Pillar i.e. by merging its provisions with the provisions from the former "First Pillar". They now form Title V (Area of Freedom, Security and Justice) of the Treaty on the Functioning of the European Union (TFEU). Title V is divided into five chapters that cover most of the issues first introduced in the EU law by the Schengen acquis: general provisions (Art. 67–76 TFEU), border checks, immigration and asylum (Art. 77–80 TFEU), judicial cooperation in civil matters (Art. 81 TFEU), judicial cooperation in criminal matters (Art. 82–86 TFEU) and police cooperation (Art. 87–89 TFEU). For most of these provisions, the following applies: ordinary legislative procedure, ordinary types of legal instruments, and full power of EU institutions including the Court of Justice of the European Union.[22] Articles 87-89 TFEU define police cooperation which will together with Schengen area be in focus of this paper.

3. INTEROPERABILITY AS THE EU TOOL FOR PROTECTION AGAINST CRIMINALITY AND ILLEGAL MIGRATIONS

It would be wrong to say, however, that interoperability has been solely introduced due to terrorist and migrant events in the EU since 2014, as the EU has previously considered how to introduce interoperability of information systems.[23] Already after 09/11 events, the EU started to develop concept of so-called "smart" borders. Proposed Entry – Exit system (hereinafter: EES) was an upgrade to the Visa Information System (hereinafter: EU VIS) presented in the Impact Assessment.[24] The proposed EES was planned to be connected to SIS in order to enable checks between two databases.

---

[18] Art. 67(3) TEC-Nice

[19] Peers, S. (2011). EU Justice and Home Affairs Law (non-civil). *The Evolution of EU Law*. Oxford University Press, p. 663.

[20] Case C-105/03, *Pupino* (ECJ 16 June 2005). See further on this matter in: Peers 2007, p. 883; Hinarejos 2009, p. 29–49.

[21] Case C-176/03, *Commission v. Council* (ECJ 13 September 2005) ; Cases C-317/04 and C-318/04, *Parliament v. Council and Commission* (ECJ 30 May 2006); Case C-440/05, *Commission v. Council*,(ECJ 23 October 2007); Case C-301/06, *Ireland v. Council and Parliament* (ECJ 10 February 2009); Case C-482/08, *UK v. Council* (ECJ 26 October 2010) See more: Peers 2011a, para 16.

[22] Duić, D. (2019). *Migracijsko pravo EU i prava djeteta // Prekogranično kretanje djece u Europskoj uniji* / Župan, M. (ur.). Pravni fakultet Osijek, 131-155.

[23] Jeandesboz, J., Bigo, D., Hayes, B., & Simon, S. (2013). *The Commission's legislative proposals on Smart Borders: their feasibility and costs*. European Parliament, 1-18.

[24] European Policy Evaluation Consortium (2004) Study for the extended impact assessment of Visa Information System. Brussels, December 2004.

In the next COMM Communication document[25] lack of pre-control of visa-exempt passengers who were was highlighted not systematically controlled before coming to the EU border.[26] In order to overcome overall challenges there was proposed creation of Registered Traveller Program (hereinafter: RTP) for low-risk people, regardless of whether or not they need a visa to enter the EU; "Automated Border Control "gates" (hereinafter: ABC gates) which would speed up the entry of *bona fide* travellers (EU citizens pre-registration program); EES that would record the arrival and departure of all non-EU citizens and the Electoral System of Travel Authorization (hereinafter: ESTA), which would allow real verification of entry conditions from all third country visa exempt nationals.[27]

COMM also prepared an Impact Assessment[28] based on two independent studies[29]. The results of this Impact Assessment indicated that the estimated cost of introducing RTP and EES would be around €113 Mio.[30]

Activities continued in 2010 with equal intensity. COMM announced in November 2010 that the entire system could be operational by 2015.[31] At the informal Justice and Home Affairs ministerial meeting in Poland[32], the states were invited to further consider the whole package in terms of costs and effects that the introduction of the new technology could have for work processes, including and data protection. All activities arouse the interest of the European Data Protection Supervisor (hereinafter: EDPS), who asked for an additional explanation on the reasons for the introduction of the power system.[33] COMM continued to insist on the introduction of the package[34], justifying everything by an operational 80% increase in air

[25] European Commission (2008) Preparing the next steps in border management in the European Union. Brussels, COM (2011) 69 final, 13.2.2008.

[26] Ibidem, p. 4.

[27] Ibidem, p.7-9.

[28] European Commission (2008) Preparing the next steps in border management in the European Union - Impact Assessment. Brussels, SEC (2008) 153 final, 13.2.2008.

[29] GHK (2007) Preparatory study to inform an Impact Assessment in relation to the creation of an automated entry/exit system at the external borders of the EU and the introduction of a border crossing scheme for bona fide travellers ('Registered Traveller Programme'), op.cit.; Unisys (2008) Entry-Exit Feasibility Study: Final Report, op.cit.

[30] SEC (2008) 153, op.cit. p. 52.

[31] European Commission (2010) Staff Working Document on the fulfilment of the 29 measures for reinforcing the protection of the external borders and combating illegal immigration adopted at the Justice and Home Affairs Council meeting, held on Brussels on 25 and 26 February 2010. Brussels, SEC (2010) 1480 final, 26.11.2010.

[32] Polish Presidency of the European Union (2011) Conclusions of the Informal Meeting of the Justice and Home Affairs Ministers in Sopot, 18–19 July 2011: Smart borders in the Schengen space (https://www.statewatch.org/media/documents/news/2011/jul/eu-council-informal-jha-smart-borders.pdf - accessed 24 October 2021).

[33] EDPS (2011) Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration, Opinion C(2011)-0445, 7 July 2011 (https://edps.europa.eu/sites/default/files/publication/11-07-07_migration_en.pdf - accessed 25 October 2021).

[34] European Commission (2011) Smart borders – options and the way ahead. Brussels, COM(2011) 680 final, 25.10.2011.

passenger traffic by 2030[35], necessity to find solution for excessive waiting at airports and increased illegal migrations.[36]

The costs of introducing EES and RTP were estimated at €1.335 million in 2011 with possible savings of up to 30% if both systems are applied on the same technical platform.[37]

During 2014, we can talk about "slowing down" of the process of introducing interoperability within the EU, but the events that followed significantly accelerated legislative and implementation activities.

The political decision-making process regarding the establishment of the interoperability of the EU systems was challenged by the external influences described in the introductory considerations. Given the importance of the changes and their complexity in further implementation, it can be said that the whole process took place relatively quickly because both the Council of the EU and the European Parliament (EP) reached a kind of "consensus" in joint action.

On 28 April 2015, COMM published European Agenda on Security (European Commission, 2015).[38] The Agenda was published only three months after terrorist attack on the reduction of satirical journal Charlie Hebdo.

It set out three priorities: developing a strong EU response to terrorism and foreign terrorist fighters; fighting serious and organised cross-border crime and fighting cybercrime. To solve these three different objectives, the agenda proposes "interoperability" as a way to guarantee the safety of populations within the EU (Bigo, Ewert, Kuşkonmaz, 2020: 11-12).

In the middle of the migrant crisis and due to incessant terrorist attacks in the EU, in April 2016 COMM presented a Communication Stronger and smarter information borders and security.[39]

The strategy clearly outlined situation, pointed out weaknesses and suggests next steps. At the same time, active systems, their weaknesses as well as proposals for the establishment of new systems were listed. For the first time, system improvements are mentioned by introducing biometrics that need to be checked through available systems. Furthermore, the need for system networking was discussed and a methodology was proposed on how to achieve it. The strategy was a good starting point, but to identify the specific shortcomings of the current situation, it was necessary to establish a working group of experts of various profiles: police officers, border guards, public prosecutors, immigration and custom officers and others to generate technical, legal and operational challenges. COMM has set up a High-level Expert Group on information systems and interoperability (hereinafter: HLEG) in June.[40] The HLEG was formally made of representatives of the COMM, Member States, associated members of the

[35] Ibidem, p. 3.

[36] Ibidem.

[37] Ibidem, p.14.

[38] https://ec.europa.eu/anti-trafficking/european-agenda-security_en - accessed 27 October 2021.

[39] COM(2016) 205 of 6 April (https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=COM%3A2016%3A205%3AFIN)- accessed 16 October 2021)

[40] Commission Decision of 17 June 2016 setting up the high–level expert group on information systems and interoperability – 2016/C 257/03 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2016.257.01.0003.01.ENG&toc=OJ%3AC%3A2016%3A257%3AFULL – accessed 16 October 2021).

Schengen area, relevant EU agencies, the European Counter Terrorism Centre (ECTC), and the EDPS, as well as representatives of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and of the general secretariat of the Council as observers.[41]

The EU Council did not hesitate to act either: as early as June 2016, it adopted the Roadmap to enhance information exchange and information management, including interoperability solutions in the JHA area.[42] As in the COMM acts, the Roadmap emphasizes "privacy and data protection are core values, fundamental rights and norms in the EU". In this Roadmap was, *inter alia,* described Framework for a more integrated EU information Architecture which states the importance of the information to be "(…) collected, checked and connected the right information at the right time in the right place to undertake effective action". Concrete objectives, actions, primary responsible party/parties, stakeholders, timetable, monitoring and Council request financial support were also listed.

The European Parliament (hereinafter: EP) in the same period has adopted a Resolution on the Commission's work program for 2017 in which the EP is called for "proposals to improve and develop existing information systems, address information gaps and move towards interoperability (…) accompanied by necessary data protection safeguards".[43]

HLEG completed its work in May 2017 when it submitted its final report. Based on the Final Report, the COMM has set up a Seventh progress report towards an effective and genuine Security Union.[44] This Report clearly emphasised shortcomings in security, border and migration management and goals to be achieved by 2020.[45] In order to address the shortcomings, actions in three areas have been proposed: maximising the benefits of existing information systems, stressing that Member States need to make full use of these systems; developing new and complementary actions to address gaps in the EU s architecture of data management and need to improve the interoperability of information systems.[46] For the first time have been mentioned: a single-search interface (SSI), shared biometric service (sBMS) and Common Identity repository (CIR).[47]

HLEG underlined unsystematic recording of the crossing of the external border by the non-EU citizens, little or no possibility of checking carriers of long-stay visas, residence permits and residence cards of third-country nationals when crossing EU borders. Role of customs authorities in interagency cooperation, especially at the external border, was emphasized.[48]

---

[41] More about the work of HLEG available in: Bigo, D., Ewert, L., Kuşkonmaz E.M., (2020). *The interoperability controversy or how to fail successfully: lessons from Europe*. International Journal of Migration and Border Studies, Vol.6, No 1-2, 15-19.

[42] https://data.consilium.europa.eu/doc/document/ST-9368-2016-REV-1/en/pdf - accessed 16 October 2021.

[43] European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission work Programme 2017 (https://oeil.secure.europarl.europa.eu/oeil/popups/printficheglobal.pdf?id=669116&l=en – accessed 16 October 2021).

[44] https://www.eumonitor.eu/9353000/1/j4nvhdfcs8bljza_j9vvik7m1c3gyxp/vkeajrssfjzk - accessed 16 October 2021.

[45] Ibidem, p.2-3.

[46] Ibidem, p. 2-3.

[47] Ibidem, p.5.

[48] Ibidem, p.6-7.

COMM stated in the document that specific data protection provisions need to be adopted and emphasized that data quality is essential for information systems to be effective.

When the COMM completed its part of the work, the Council of the EU took the stage and at the Council meeting on Justice and Home Affairs on 8 and 9 June 2017 again invited the COMM to prepare, as soon as possible, a draft legal act to shape HLEG's decisions. Soon after, COMM announced concrete measures in the context of the 2018 Work Program.[49]

In drafting the proposal for a legal act,[50] the Council had to create two Regulations which would serve as legal bases for the introduction of the interoperability: one in the field of police and judicial cooperation, asylum and migration[51] and the other in the field of borders and visa.[52]

This distinction was introduced because the legal bases, the scope and the field for the implementation of both Regulation, are different. The legal basis follows the logic of the TFEU. For the Regulation 2019/817 the provisions of Art. 77 and Art. 79 TFEU are relevant. Irregular migration and irregular stays are governed by Art. 79.

Articles 82 and 85 TFEU are regulating cooperation in criminal matters. For the police cooperation are of the relevance Art. 87 and 88. Data handling which is prescribed in the Art. 87(2) (a) is of the special importance since it is mentioning "collection, storage, processing, analysis and exchange of relevant information".[53]

If we look further into the content of the EU interoperability Regulations, it is notable that the systems referred to in Regulation 2019/817 (EES, VIS, ETIAS and SIS) are aimed at protecting the crossing of the EU's external border. In contrast, Regulation 2019/818 is focused on "detection and investigation of terrorist offences and of other serious criminal offences".

What meaningfully connects both Regulations are aim and objectives. The provisions of both Regulations defining the Aim[54] and Objectives[55] are substantively identical, indicating that the legislator was focused on establishing a single, interoperable system, the introduction of which was explained in an identical manner.

---

[49] COM (2017) 650 final (https://www.eumonitor.eu/9353000/1/j4nvhdfcs8bljza_j9vvik7m1c3gyxp/vkiqnh38o5zz- accessed 16 October 2021).

[50] The whole process is described in details on: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0793 (accessed 16 October 2021).

[51] Regulation (EU) 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. OJ L135/85.

[52] Regulation (EU) No. 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 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA. OJ L135/27.

[53] CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION (2012), OJ C326/47, available on https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF – accessed on 19 October 2021.

[54] Regulation 2019/817 and Regulation 2019/818, Preambule, para 9.

[55] Regulation 2019/817 and Regulation 2019/818, Preamble, article 2.

Interoperability regulations regulate practical application as a future event.[56] In relation to Eurodac, Regulations will be applied when the recast of Regulation (EU) No 603/2013 becomes applicable.[57] Provisions of Regulations related to the shared BMS, ESP, CIR and MID shall apply once the eu-LISA has declared the successful completion of comprehensive tests of all systems and has validated the technical and legal arrangements to collect and transmit the data.[58] Provisions on automated data quality control mechanism and procedures, the common data quality indicators and the minimum data quality standards as well as provisions on CRRS will be implemented by the COMM's implementing act, which will be submitted once the eu-LISA declares successful completion of comprehensive tests.[59] The adoption of the implementing act is pending an approval or tacit confirmation by the European Parliament and the European Council.[60]

4. PNR AND DATA PROTECTION CONSTRAINS

In order to understand the overall context around the interoperability of the EU system, it is certainly necessary to make some observations on Passenger Name Record (hereinafter: PNR) Directive.[61]

As early as 6 November 2007, COMM drafted a Council Framework Decision on the use of PNR data,[62] which was submitted to the Council's working groups for discussion. Following the entry into force of the TFEU on 1 December 2009, it was more applicable. With the entry into force of the Lisbon Treaty, Framework Decision ceased to be implemented.[63]

The European Agenda on Security issued on 23 September 2015[64] is mentioning "Passenger Name Record (PNR) system for airline passengers that is fully compatible with the Charter of Fundamental Rights while providing a strong and effective tool at EU level". It is further noted that "Analysis of PNR information provided at the time of booking and check-in will help to detect (…) high risk travellers previously unknown to law enforcement

---

[56] Art. 75 of the 2017/818 Regulation and Art. 79 of the 2017/817 Regulation.

[57] Art. 79 of the 2017/817 Regulation.

[58] Art. 72 of the 2017/817 Regulation and Art. 68 of the 2017/818 Regulation.

[59] Ibidem, para 5 and 6.

[60] Article 73 of the 2019/817 Regulation and art. 69 of the 2019/818 Regulation.

[61] DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L119/132.

[62] Petrašević, T., Duić, D. (2016). *Direktiva o evidenciji podataka o putnicima (PNR) i zaštita podataka u EU*. Zbornik radova 5. Međunarodne znanstveno-stručne konferencije „Unaprjeđivanje sigurnosne uloge policije primjenom novih tehnologija i metoda" / Vukosav, Joško; Butorac, Ksenija; Sindik, Joško (ur.) Zagreb: Ministarstvo unutarnjihposlova Republike Hrvatske, Policijska akademija, 647-648.

[63] More about amendments in Lisabon Treaty available in: Đurđević, Z. (2008). *Lisabonski ugovor – prekretnica u razvoju kaznenog prava u Europi*. Hrvatski ljetopis za kazneno pravo i praksu, 15 (2), 1077-1127.

[64] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, The European Agenda on Security, COM(2015) 185 final, Strasbourg, 28.4.2015 (https://ec.europa.eu/anti-trafficking/european-agenda-security_en - accessed 21 October 2021).

authorities".[65] Finally, the PNR Directive should contribute to identify high risk travellers in the context of combat terrorism, drug trafficking, trafficking in human beings, child sexual exploitation and other serious crimes. Like interoperability, PNR also contributes to reducing security gaps in the EU. The legislative process of passing the Directive has significantly accelerated after the migrant crisis and terrorist attacks in 2014 and 2015. As mentioned, Directive has been in the process of adoption before 2015 for a long time.[66] The Directive has caused a lot of controversy, especially in terms of collecting personal data on passengers, storage periods, methods of exchange, safety measures regarding records of personal data etc.[67]

Like in the future implementation of interoperability, in the implementation of PNR we are considering issue of processing a larger amount of personal data available to Law Enforcement. In contrast to the interoperability which is, as explained in the Chapter 3, still not completely in the implementation phase, PNR is accompanied by several important judicial decisions that primarily relate to the issue of adequately regulated storage, exchange and protection of personal data. Whenever big data set is subject to a processing, principle of proportionality, as one of the main principles of the EU law,[68] appears to be considered. Principle of proportionality requires that the undertaken measures are proportionate to their objectives and the freedom of individuals is not restricted beyond what is necessary to the public interest.[69] Proportionality is one of the basic principles of EU law, for which it can be said that there is almost no sphere of social life to which it could not be applied.[70]

The principle of proportionality is one of the most important principles that has been developed in TEU. Article 5 (4) TEU discusses how "action shall not exceed what is necessary to achieve the objectives of the Treaties." If EU law has been applied in several ways, the principle of proportionality requires that the assessment does not go beyond what is necessary to achieve the objectives of the TEU.[71] There are three main categories of cases that might be challenged on grounds of proportionality: when the individual argues that the policy choice is disproportionate, when the rights of individuals have been restricted by Union action and the cases where the penalties imposed are too excessive.[72]

In the *Case C-275/06, Promusicae*, *Música de España (Promusicae) y Telefónica de España* SAU,[73] the Court of Justice of the EU stated that it is indisputable that the provision

---

[65] Ibidem, p.7.

[66] On 3 February 2011, the European Commission published a Proposal for a Directive on the use of passenger records for the prevention, detection, investigation and prosecution of terrorist offenses and serious crime (EU PNR Directive, 2011/0023 COD). For a long time, the Council sought to launch negotiations with the European Parliament. Although adoption was delayed, significant EU funding was available to countries to establish their own PNR. The UK was the first country, then still in the EU, to establish its own PNR unit.

[67] Petrašević, T., Duić, D. (2016), 647-651.

[68] Groussot, X. *General Principles of Community Law*. Europa Law Publishing, Groningen, 2006, 145.

[69] Tridimas, T. (2006). The general principles of EU law, Oxford University Press, 136.

[70] C-120/94 Commission of the European Communities v Hellenic Republic, [1996], ECLI: EU:C:1996: 116, Opinion of Advocate General Jacobs, para. 47. (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61994CO0120&from=EN - accessed on 2 November 2021).

[71] Craig, P.; de Burca, G. (2020). *EU Law, Text, Cases and Materials*, Oxford University Press, seventh Edition, 583.

[72] Ibidem, 584, 586 and 588.

[73] https://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06 - accessed on 28 October 2021.

of names and addresses of individuals includes the provision of personal data, i.e. information concerning identified or identifiable natural persons, as defined in Article 2a of Directive 95/46 / EC. Such provision of information constitutes the processing of personal data in accordance with Article 2 (1) of Directive 2002/58, in conjunction with Article 2 (b) of Directive 95/45 / EC. (Petrašević, Duić, 2016: 645). The court, questioning the plaintiff's request regarding the provision of data on users of teleoperator services that he would later use in civil proceedings, pointed out that "(…) Member States may adopt legislative measures to restrict the scope *inter alia* of the obligation to ensure the confidentiality of traffic data, where such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offence or of unauthorized use of the electronic communications system, as referred to in Article 13 (1) of Directive 95/46".[74] Further on, decision emphasised that "the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided. However, it does not follow from those provisions that they require the Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.[75] Finally, court has decided that the EU Law does not "require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings."[76] . At the end it, nevertheless, expresses that the "Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality."[77]

In the *Case C-101/01 Criminal proceedings against Bodil Lindqvist*,[78] it has been established that the provision of personal data of various persons and their telephone numbers, information about their employment or about their hobbies on the website represents the processing of personal data. Discussing, *inter alia*, whether the public disclosure of personal data on the internet constituted a breach of Directive 95/46, the Court took the position that any sanction for an alleged breach should respect the principle of Proportionality and that the penalty should be assessed according to the circumstances of each case and in particular with duration of the breach and the importance, for the persons concerned, of the data disclosed.[79]

---

[74] Case C-275/06, para. 49.

[75] Ibidem, para.58.

[76] Ibidem, para.70.

[77] Ibidem, para. 71.

[78] https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-101%252F01&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=en&avg=&cid=32316418 – accessed on 27 October 2021.

[79] Petrašević, T., Duić, D. (2016). Direktiva o evidenciji podataka o putnicima (PNR) i zaštita podataka u EU. Zbornik radova 5. Međunarodne znanstveno-stručne konferencije „Unaprjeđivanje sigurnosne uloge policije primjenom novih tehnologija i metoda" / Vukosav, Joško; Butorac, Ksenija; Sindik, Joško (ur.) Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija, 645.

The consequences of the transfer of incorrect data can have unforeseeable consequences. A good example is the treatment of Syrian and Canadian citizen Maher Arar, who, based on apparently inaccurate information provided by the Canadian authorities to the American side, was returned from the United States to Syria in September 2002. After more than a year in custody, Arar was released in October 2003. It was not until 2006, based on the findings of an investigation by federal bodies, that he was cleared of any suspicion of any connection to terrorism.[80]

One of the key cases in the US legal praxis on the implementation of PNR was *Gordon v. FBI*, 388 *F. Supp. 2d 1028 (N.D. cal 2005)*[81] stating that the list of passengers must be shown to passengers in case. Court found that agency did not adequately explain how release of "the legal basis for detaining someone whose name appears on a watch list could be used to circumvent agency regulations".

In the case *Rahinah Ibrahim v. U.S. Dept. Of Homeland Security, No. 14-16161 9th Cir. 2017* has been established that the professor form Malesia Rahinah Ibrahim was put on the watch list by an official who carelessly filled in one form.

Another relevant judicial decisions on the usage and detention of PNR data is Court's *Opinion 1/15* on *the PNR (Passenger Name Record) Agreement between EU and Canada.*[82] Decision is focused on the border management policy of PNR namely on the establishment of the infrastructure for data sharing between the EU and Canada. Main principles of the PNR are quite like those established for the EES: recording personal data of everyone willing to cross the border and giving access to these data to the law enforcement community (Napieralski, 2019: 2). In this case Court was of the opinion that it is acceptable, related to the EU – Canada PNR Agreement, to retain data of all passengers, regardless of their link to a specific threat, during their stay in Canada.[83] Further on, Court was of the opinion that, in order to prevent discrimination, data retention should be implemented towards all travellers between the EU and Canada.[84]

There is an interesting opinion of Advocate General Mengozzi who took a view that certain provisions of the agreement were contrary to the EU Charter of Fundamental Right. Moreover, principle of proportionality was described as the "fair balance between the legitimate desire to maintain public security and the equally fundamental right for everyone to be able to enjoy a high level of protection of his private life and his own data".[85]

In the Case C-311/18 Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (hereinafter: Schrems II case)[86], activist Maximilian Schrems posed

---

[80] Guild, E. (2007). *Inquiry into the EU-US Passenger Name Record Agreement*. CEPS Policy Brief, No. 125, p. 1-3.

[81] https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption7e_0.pdf - accessed 27 October 2021.

[82] Opinion 1/15 of the Court on the Draft Agreement between Canada and the European Union (Passenger Name Records) [2017] ECLI:EU:C:2017:592.

[83] Ibidem, para 197.

[84] Ibidem, para 232.

[85] https://eclan.eu/en/eu-case-law/opinion-1-15-eu-canada-pnr-agreement- accessed on 03 November 2021.

[86] https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=37104984 – accessed on 03 November 2021.

request to Irish data Protection Commissioner to invalid the Standard Contractual Clase (legal bases for personal data transfer between the EU and United States) for Facebook's transfer of personal data from the EU to the headquarter in the United States (hereinafter: US). Data transferred to the US,[87] as argued, were available to the US intelligence agencies which is, as claimed, violation of the main rule of data protection that the transfers outside of the EU and EEA are prohibited unless an adequate safeguard is used.[88] Regarding principle of proportionality, Court took a position that "(…) the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary".[89]

Further on, the Court states that the US authorities did not meet the standards of protection of human rights relating to EU citizens, which has called into question adequate level of data protection.[90]

Finally, the Court has decided that, unless there is a valid COMM adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country if the EU standards on data protection are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, cannot be ensured by that third country.[91]

In conclusion, in PNR judgments, the court has generally questioned the application of the principle of proportionality. The transfer of data to third parties is possible only if in that third party to which the data is transferred there are prescribed clear and precise standards of protection of personal data against misuse in each individual case as well as in EU countries. In the search for an answer to the question of what is considered personal data, by analogy with the application of *Case C-101/01 Criminal proceedings against Bodil Lindqvist,* it is to be assumed that the term will be interpreted broadly.

In the Regulations on the Interoperability is clearly stipulated implementation of the principles of proportionality from Art. 5 of the TEU and necessity that the implemented measures "do not go beyond what is necessary in order to achieve (…) objectives".[92] In the future application of interoperability, the court is expected to question the application of the principle of proportionality.

---

[87] See more in: Chander, A. (2020). Is Data Localisation a Solution for Schrems II, Journal of International Economic Law, Georgertown University Law Center, p.2-4. (https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3318&context=facpub - accessed 03 November 2021).

[88] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation) (OJ 2016 L 119, p. 1; 'the GDPR'), art. 45.

[89] Case C-311/18, para. 176.

[90] Ibidem, para. 178.

[91] Ibidem, para. 203.

[92] Preamble, para. 68 of the 2019/817 Regulation and Preamble, para 64 of the 2019/818 Regulation. See also art. 2(f) of both Regulations.

The PNR Directive is a response to the terrorist attacks in Paris in November 2015 but, is potentially problematic in terms of the freedom of movement of EU citizens and poses a challenge to the rule of law, in particular the right to protection of personal data.[93] PNR introduces substantial verification and control of the movement of EU citizen with collection of sets of personal data that are collected. The question arises as to whether the prescribed measures are necessary, proportional and harmonised with the fundamental principles of collection and processing of personal data.[94]

According to some authors, systematic monitoring of the movement of EU citizens based on "risk categories" represents violation of the principle of "non-discrimination" in relation to those EU citizens who have another, "foreign" citizenship. The application of the so-called "Person-centric" approach by which measures are directed towards a specific person, might lead to violation of the principles of the EU Charter of Fundamental Rights.[95]

5. EU INFORMATION SYSTEMS

5.1. Description of the EU Interoperable Systems

Specific objectives of the Interoperability can be summed up under access to the information by the competent authorities (border guard, law enforcement officers, immigration officers and judicial authorities), setting up of the solution which will enable detection of multiple identities linked to the same set of biometrics data, with the purpose to identify identity frauds; facilitate identity checks of the third country nationals and finally, to reinforce access by the law enforcement authorities to non-law enforcement information systems where necessary for the prevention, detection or prosecution of serious crime and terrorism.

Interoperability may be defined as a "characteristic of a product or a system, whose interfaces are completely understood, to work with other products or systems, at present or in the future, in either implementation of access, without any restrictions. The concept of Interoperability differs from neighbouring concepts like integration, compatibility or portability. Integration happens when two or more functions or components of the same system interact. Compatibility occurs 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" (Oliveira, 2019:2).

---

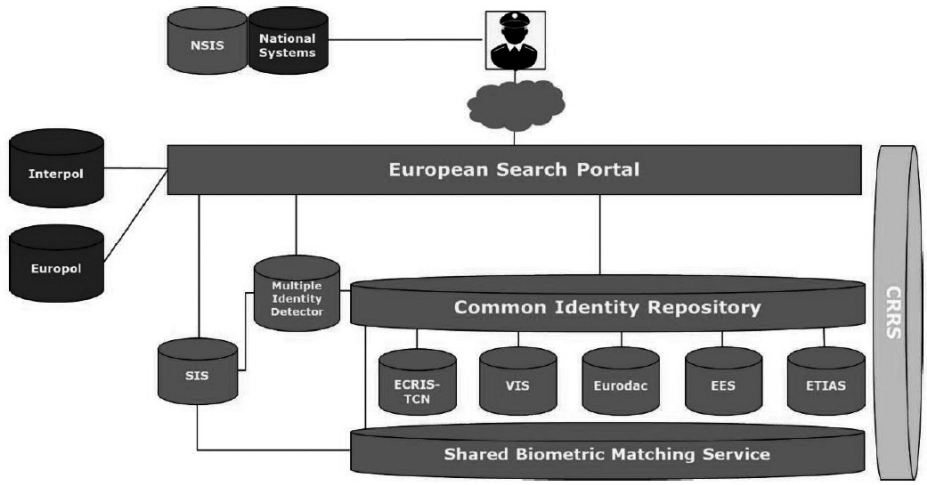
[93] Pejaković- Đipić, S., Karas, Ž. (2018). *Neki problem kod prikupljanja i razmjene podataka o putnicima u zračnom prometu*. Policija i sigurnost, 27 (4), 444-445.

[94] Bigo, D., Brouwer, E., Carrera, S., Guild, E., Guittet, E., Jeandeboz, J., Ragazzi, F., Scherrer, A. (2015). *The EU Counter-Terorism Policy Responses to the Attacks in Paris, Towards an EU Security and Liberty Agenda*. CEPS Paper in Liberty and Security in Europe, No. 81, p. 2.

[95] Ibidem, p. 12.

Interoperable solution is foreseen to function as described in Figure 2.

Figure 1: Interoperable solution of different EU databases (Jokhadze, 2020: 22)



In order to be able to clarify the interdependence of the system, it is necessary to clarify in more detail the role of each individual system.

The Regulation on Entry Exit System (hereinafter: EES) was set up in 2017.[96] Its purpose is to monitor the entry / exit of *bona fide* travellers, identify persons with a visa that exceed the allowed time of stay and enable law enforcement to monitor the history of entry and exit into the EU for each individual person, visa holder.[97] The power system will replace the stamp upon entry into the country and is supported by the EU VIS[98] which does not automatically record a person's actual entry into the EU. The system records alphanumeric and biometric data; family name, given names, date of birth, nationality or nationalities, sex, type and number of the travel document(s), three-letter code of the issuing country, date of expiry of the validity of the travel document(s) and facial image.[99] Both visa holders and visa exempt Third country nationals (TCN) will have their data in the EES. Visa exempt TCN will be obliged to provide their fingerprints at the border, while the visa holder's fingerprints will

[96] Regulation (EU) 2017/2226 of the European Parliament and of the Council 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.

[97] Blasi Casagran,C. (2021). *Fundamental Rights Implication of Interconnecting Migration and Policing Databases in EU*, Human Right Law Review, Oxford University Press, p. 2-3.

[98] Napieralski, A. *Collecting Data at EU Smart Borders: Data Protection Challenges of the New Entry/Exit System.* Juridikum. Zeitschrift für Kritik, Recht, Gesellschaft (2019) vol. 2, pp. 202-203.

[99] EES Regulation, art. 16-17.

be available via EU VIS. EES is going to be one of the most powerful systems in terms of available data. According to the Commission: 'the total number of regular border crossings in 2025 is forecast to rise to 887 million, of which around one-third are expected to be done by third-country nationals traveling to Schengen countries for a short- term visit".[100] Estimation was made before Brexit and at that time already reached almost 300 million people who will be affected by the EES.

The power system should function like Trusted Traveler programs in the USA[101] in a way that would introduce "Kiosk" that would allow passengers to pass through. When passing the Kiosk, passenger's biometric and biographical data will be automatically controlled. The system would immediately signal whether a person has exceeded the allowed time of stay to border guards, whether there are previous entry bans and would automatically register further allowed time of stay. Before arriving at the border control, the person would first go through a face recognition system and fingerprint check. Preliminary tests conducted in Germany show that check-in times for passengers using Kiosks would be significantly reduced: by 53 seconds on average for visa-exempt TCN to enter the EU and 82 seconds compared to passengers who need a visa to enter the EU.[102]

Earlier than the EES, in 2004 was established EU **Visa Information System (EU VIS)**[103] with the aim of joint monitoring of all short-stay visa applicants for up to 90 days. The system was established to speed up the visa process, prevent so-called "visa shopping", to promote the fight against fraud, to enable the identification of persons barred from entering the EU, to promote joint control of the external border of EU countries, the implementation of common goals of Dublin II Convention and to prevent the internal security of the Member States.[104] The comparison of data stored in the EU VIS against data stored in other information systems and databases should be automated. If such a comparison reveals the existence of a correspondence, known as a 'hit', between any of the personal data or combination thereof in an application and a record, file or alert in those other information systems or databases, or with personal data in the ETIAS watch list, the application should be verified manually by an operator from the competent authority. The assessment of hits performed by the competent authority should be considered for the decision whether to issue a short-stay visa, a long-stay visa or a residence permit. The 2021/1133 Regulations *de jure* integrated VIS into interoperability. In the legislative sense, scope of the Regulation is extended to long-stay visas and residence permits holders, age of the inclusion to the system has been decreased from 14 to 6 years old and includes facial image and two fingerprints of the holder.[105]

---

[100] Explanatory Memorandum of the Proposal for the EES Regulation COM/2016/0194 final - 2016/0106 (COD).

[101] 'Trusted Traveler Programs'. US Department of Homeland Security (https://ttp.dhs.gov - accessed on 26 October 2021).

[102] Steffens, F. (2020). *Facing up to the New World of Border Control*, Biometric Technology Today, Issue 9, p. 8-9 (https://www.sciencedirect.com/science/article/pii/S0969476520301235 - accessed on 26 October 2021).

[103] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences [2008] OJ L218/129.

[104] Blasi, (2021), op. cit. p. 3.

[105] Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU)

European Travel Information and Authorisation System (hereinafter: ETIAS)[106] should allow for the advance collection of travel data of persons, visa – exempt third-country nationals. The system records alphanumeric and biographic data inserted by persons *via* application. It is introduced, *inter alia*, as an obligation for visa-exempt third country nationals to announce their arrival in the EU.[107] Studies on the estimation of the number of ETIAS passengers have not been carried out since the UK left the EU. However, there are studies on the preparation of the so-called package on Smart Borders.[108]

Eurodac system, which was set up in 2003,[109] establishes a system according to which the state in which the asylum seeker first applied for asylum is responsible for the reception and processing of the asylum seeker's application. Eurodac stores data asylum seekers (Category 1 data), individuals connected with irregular border crossings (Category 2), and third-country nationals or stateless persons found to be irregularly staying in the Member States (Category 3). Article 20 of the EURODAC Regulation foresees three conditions to be granted access to the database: when it is necessary for the prevention, detection or investigation of terrorist offences or of other serious criminal cases; when it is necessary in a specific case; and if there are reasonable grounds to believe that comparison will contribute to the prevention, detection or investigation of the crime at hand, in particular where it is suspected that the offender falls under the EURODAC Regulation threshold. EURODAC includes fingerprints, gender, date of fingerprint taking and the reference number of the country where the fingerprints were taken.[110] EURODAC is one of the most sensitive systems for accessing by Law Enforcement because it stores, *inter alia*, data on asylum seekers. EDPS pointed out in 2012[111] that it does not support the "function creep approach" according to which the purpose of reviewing this database would be expanded without clear legal and factual clarification.

2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System [2021] OJ L248/11.

[106] REGULATION (EU) 2018/1241 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS) [2019] OJ L236/72.

[107] Quintel, T. (2018). *Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention*, University of Luxembourg Law Working Paper No. 002-2, p.8.

[108] https://www.eulisa.europa.eu/Publications/Reports/Smart%20Borders%20-%20Technical%20Report.pdf – accessed 17 October 2021.

[109] Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (the "Dublin II Regulation"). 2003.OJ L 50/1.

[110] Roots, L. (2015) 'The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination' Baltic Journal of European Studies, Vol.5, No. 2, 111.

[111] Ibidem, p.118-121.

From 2016, a proposal is being made according to which data would be stored in the system for 5 years, the age limit would be lowered from 14 to 6 years for persons from whom data should be excluded in all three categories, and the establishment of facial recognition software is planned.[112]

Schengen Information System (hereinafter: SIS) is the largest EU database in general, which according to official EU-Lisa statistics at the end of 2020 contained 93 million data.[113] It is the starting point for searches for persons and objects in the EU and the starting point for the work of Law enforcement and migration purposes.[114] The specificity of SIS II is that it mainly focuses on TCN but also on EU citizens who are suspected, have committed, or are sentenced for committing serious crimes and terrorism. Furthermore, the system stores data on objects too. After the revision of Schengen Border code, it is also used for checking of the external EU border by the EU citizens on the non-systematic way.[115]

SIS II has also its disadvantages like lack of data quality in some situations and limited data accessibility. The system has been significantly upgraded 2018[116] with new features like collecting biometric data such as fingerprints and the DNA profiles. In addition, the system contains all return decisions issued by national authorities and offenders DNA profiles.

European Criminal Records Information System for Third Country Nationals (hereinafter: ECRIS – TCN)117 is a centralized system whose purpose is to share data on

---

[112] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), 4 May 2016, COM (2016) 272 final. See also New Pact on Migration and Asylum documents adopted on 23 September 2020 available on: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/new-pact-migration-and-asylum_en (access on the 25th of April 2022).

[113] SIS II – 2020 statistics, EU-lisa, March 2020 – available on: https://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20-%202020%20Statistics%20-%20report.pdf (access on the 18th of October 2021), p.11.

[114] Rošić, M. (2014). *Najznačajniji aspekti međunarodne policijske suradnje Republike Hrvatske s državama* članicama *Europske Unije* (The Most Significant Aspects of International Police Cooperation of the Republic of Croatia with the EU Member States). Hrvatski ljetopis za kazneno pravo i praksu. 21(2), p. 297-301.

[115] Glouftsios, G., Bellanova, R. (2020). *Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintanance*. Geopolitics, 4-6.

[116] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 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 and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006; Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals [2018] OJ L 312/1.

[117] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country

legally convicted persons, third-country nationals. The whole assumption of the ECRIS-TCN is that third country nationals are a greater security risk including in respect to terrorism than nationals of the Member States. Embedded in the logic of ECRIS-TCN is the presumption that the privacy of Non- EU citizens is less protected in terms of human right protection than that of EU citizens (Bigo, Ewert, Kuşkonmaz, 2020: 15). The system is a great help to judicial bodies (judges, prosecutors) on tracing criminal history of the sentenced persons, regardless of the country of conviction.[118] Mandatory data are identity document and biometric data of the person. The system is expected to be operational until the end of 2022.

5.2. Interoperability Components

European search portal (hereinafter: ESP), serves as one-stop shop enabling end-users (or central systems) to simultaneously query several systems in parallel.[119] The ESP chooses which type of user can check which kind of information. It enables queries of Interpol[120] and Europol data too.

The **shared biometric matching service (hereinafter: sBMS)** enables comparison of biometric data based on biometric templates of fingerprints and facial images across different EU information systems.[121]

The **common identity repository (hereinafter: CIR)** is a shared container of biographical and biometric information, such as name, gender and date of birth, stored in the EES, ETIAS, VIS, Eurodac and ECRIS-TCN. CIR also enables the identification of third-country nationals in the territory of the Member States (Article 20 of the Interoperability Regulations). In a specific case, where there are reasonable grounds to believe that consultation of EU information systems will contribute to the prevention, detection investigation of terrorist offences or other serious criminal offences, Member States law enforcement authorities and Europol may consult the CIR in order to obtain information on whether data on a specific person are present in the EES, VIS, ETIAS or Eurodac (Article 22 of the Regulations).[122] Some authors are of the opinion that the CIR might be abused in a way that the identity checks will be done based on somebodies race or appearance.[123]

The fourth component of interoperability is the **multiple identity detector (hereinafter: MID)**, a technical component allowing for the detection of **multiple or fraudulent identities**.

nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 [2019] OJ L135.

[118] Blasi Casagran (2020), op.cit. 437.

[119] Ibidem, 438.

[120] Interpol's Stolen and Lost Travel Documents (SLTD) database and Interpol's Travel Documents Associated with Notices (TDAWN) database.

[121] Supra at 90, 439.

[122] Ibidem, 440.

[123] Ibidem, 453.

MID will detect a possible link, determine the type of link "colouring"[124] each situation differently. MID will also store the link for future use and, the most important, MID will automatically conduct checks when the new data are added in one of the systems which has data stored in the CIR or added in SIS. Thus, MID serves to detect identity fraud, multiple *bona fide* identities of travellers and false positive cases.

Central Repository for reporting and Statistics (hereinafter: CRRS) will be created in order to enable the creation and sharing of reports with statistical data for policy, operational and data quality processes.

The entire interoperability architecture should be put into production by the end of 2023.

The system as a whole is well-designed to allow interoperability of data into one whole. On the one hand, it is primarily person-centric oriented and on the other hand, it is mostly TCN-oriented. It is important to point out that since the beginning of the development of the system, the EU has gone through Brexit, which will certainly significantly increase the numbers of TCN. Due to the complexity of its application in the same way in all EU Member States, a number of other material and technical challenges can certainly be expected before the start of practical implementation, of which the real situation is best known to eu-LISA. What the legal challenges might be, we can judge now through the application of PNR.

5.3. Practical Future Scenarios

Imagine a situation in 2016 where person AB, a citizen of non-EU country C, is applying for a visa to enter country D, an EU member state. The same person duly attaches to the visa application personal data, data on the planned trip, fingerprints and photo that are all entered in the EU VIS. Person AB, after checking through the available systems (SIS, Interpol), duly obtains a visa to enter country C. Upon entering country C, the person moves freely within the entire Schengen area. Meanwhile, AB contacted other persons within Schengen area in order to commit organized criminal activities. At that point, it's hard to trace that person anymore because he is freely moving within the EU.

After full implementation of the interoperability, this situation should be prevented from the outset. In 2016 the EES Regulation established that that the EES and VIS systems can be fully interoperable in order to provide visa application history of third-country nationals by adding information on how they used their visas. The MID will make it easier to detect multiple identities and counter identity fraud. The detector will automatically notify the visa-processing in application if the applicant is known under different identities so that the authority can take the appropriate course of action. Once new information systems have become operational and interoperability between them has been ensured, the possibilities for visa-processing officers to perform quick background checks will be considerably improved.

[124] "Yellow" signs that the link may exist, manual verification will lead to maintaining the link with different colours. "Green" signs that there are the same of very similar biographical identities with different biometric data. "Red" signs that there are different biographical identities which are linked to the same biometric data and manual verification determines that this is unlawful (identity fraud). "White" signs existence of the same biometric data and the same (or very similar) biographical data (same person in multiple systems) or existence of the same biometric data but lawfully differing biographical data after manual verification.

The ESP will enable single searches to receive results from different systems. This will help to increase the security of the area without internal border controls. New VIS Regulation has included obligation on visa authorities to automatically consult the multiple-identity detector as well as other databases when conducting security and migratory assessments of third country nationals applying for a short-stay visa. Furthermore, the VIS will automatically check Europol data. In accordance with data protection standards, Law enforcement will have access to so-called non-Law enforcement databases (VIS, EES, ETIAS and EURODAC) at all steps. In the first step, the check receives a hit / no hit response in the CIR (which contains identities from VIS, EES, ETIAS and EURODAC). In case of a hit, law enforcement officers will perform the second step by accessing to the source system. The whole procedure must be in line with the EU standards on protection of fundamental rights.

Imagine a situation in which a person fills out their ETIAS application to go through Croatia to Austria mentioning visit to the relatives as the reason for issuance of the ETIAS approval. Imagine that the person is a suspect in proceedings involving Europol. In accordance with Art. 18.2a of the Europol Regulation, all data will be automatically searched by ETIAS. A person is most likely to be prevented from entering the EU, treated in accordance with the instructions of the country in which the person poses a security risk.

The situation is similar regarding ETIAS when we talk about the establishment of the so-called Watch list. States will certainly prepare criteria according to which, given the previously defined criteria, individuals will not be allowed to enter the EU.

What if such individuals still decide to come to the EU using someone else's identity (names and surnames but with their own biometric data)? In this case it helps CIR which will contain an individual file including identity data (alphanumeric and biometric) and ID documents data for each person that is registered in EES, VIS, ETIAS, EURODAC or ECRIS-TNC. Via MID will be crosschecked data in CIR and SIS. In practice, it means it will be much easier and faster to establish real identity of the „fraudster".

Apart from the purpose of preventing and preventing terrorism and organized crime, the purpose of introducing interoperability is also to prevent illegal migration. Under conditions of interoperability, for example, a 13-year-old child caught illegally crossing the EU border will be stopped, his/her identity documents, if available, checked and he/she will be photographed and fingerprinted. After entry, the Border Guards will be able to check whether the person has been criminally registered (ECRIS-TCN), whether the person has previously applied for asylum (EURODAC), how many times the person has previously entered the EU, whether there is an active search for the person. If one of the databases is positive, for example it is determined that a person has been denied asylum in an EU country, the person will be readmitted to the third country closest to the place of detention at the external border.

This raises the question of whether the overall access to data in real time is in conflict with privacy and data protection rights, the non-discrimination principle, and the protection of children, which are guaranteed by the EU Charter of Fundamental Rights, Treaty of Lisbon and the general principles of EU Law. Fully functional interoperability system should be subject to proportionality test in order to establish whether the measure have a legitimate aim, are they suitable for attaining that aim. Finally, they must not go beyond what is necessary to attain the aim, taking into account the individual's interest in exercising the subjective rights invoked but also the general interest.[125]

[125] See also: Blasi Casagran, C. (2021). Fundamental Rights Implication of Interconnecting Migration and Policing Databases in EU, Human Right Law Review, Oxford University Press, 443-452.

6. CONCLUSION

By introducing the interoperability of the EU system, the EU has entrusted the strengthening of security to the balance between protecting the rights of the individual and overcoming the threat of terrorism, general security and migratory pressures. The described terrorist threat and the strengthening of migratory pressure have led to the legislative process of introducing interoperability being implemented relatively quickly. The introduction of interoperability focused primarily on the TCN and the EU external border will certainly lead to an additional workload at all EU external borders, especially at the beginning of implementation and especially at very frequent border crossings. Experiences of using the SIS II system so far, as the most complex and most used system in the EU, show that mistakes in practical application are inevitable. Errors are mostly generated by inadequate data updates and inability to access real-time data due to technical problems.

Any such delay will very likely cause major delays at the external borders and significantly affect economic flows, especially at the external land border.

The processing of a large set of data always causes controversy over the transmission, storage, updating, access and legality of the exchange of such data with third parties and for the purposes of proceedings in EU countries. Experiences of PNR application in the EU and in the USA indicate that individual errors in application are inevitable. Depending on the severity of the consequences, such errors could have judicial epilogues.

The case law in the implementation of PNR shows that courts generally question the application of the principle of proportionality when processing a large set of data. According to the current case law in the application of PNR, the interoperability regulations and its practical implementation will be subject to the principle of proportionality in relation to the measures taken (can the same purpose be achieved by applying "weaker" measures), in relation to the availability of data (whether all Law Enforcement is indeed authorized to access all data), in relation to data retention periods and in relation to the exchange of data with third parties. Judging by the Schrems II judgment, the exchange of data with third countries will always be the subject of a careful analysis of the legislation of those third countries in each specific case.

Access to the data and the purpose of their further use by Law Enorcement are disputed, especially in relation to vulnerable groups of asylum seekers or persons in the international protection system. The court epilogue could also have cases of persons who in the meantime have acquired the citizenship of some of the EU countries and have previously been recorded several times through various interoperable systems where the deadlines for storing "old" data could be questionable.

The legislative solution in the application of interoperability is, with the exception of the SIS II system, focused on TCN. If the objectives set by the Interoperability Regulations 2019/817 and 2019/818 were really to be met, EU citizens should have been included in the application in the part of automated verification of biometric data of convicted persons. As some EU countries do not have biometric data of their citizens even after obtaining personal documents, it was necessary to introduce the obligation to issue biometric travel documents for all EU citizens until a certain period of time, which would coincide, with the start of interoperability. Finally, the reliability of the information side of the interoperability application remains questionable (failures, delays in updating data, power outages, insufficient or no signal to connect to the system, etc.) on which preliminary estimates can be made after the system is put into production.

LITERATURE

Books and articles

1. Alegre S.; Jeandesboz J.; Vavoula N. (2017) 'European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection'. PE 583.148 http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583148/IPOL_STU(2017)/58314 8_EN.pdf – (accessed 17 October 2021).
2. Baldwin-Edwards, M. / Haberton, B. (1994). *Will SIS be Europe's Big Brother*, in Anderson, M. / Den Boier, M. (eds). (1994). Policing Across National Boundaries,London/New York: Pintzer. (1994), 133-157.
3. Bigo, D., Ewert, L., Kuşkonmaz E.M. (2020). *The interoperability controversy or how to fail successfully: lessons from Europe.* International Journal of Migration and Border Studies, Vol.6, No 1-2, 1-41.
4. Bigo, D., Brouwer, E., Carrera, S., Guild, E., Guittet, E., Jeandeboz, J., Ragazzi, F., Scherrer, A. *The EU Counter-Terorism Policy Responses to the Attacks in Paris, Towards an EU Security and Liberty Agenda*. CEPS Paper in Liberty and Security in Europe, No. 81, p. 1-17.
5. Blasi Casagran, C., (2021). *Fundamental Rights Implication of Inerconnecting Migration and Policing Databases in EU*, Human Right Law Review, Oxford University Press, 433-457.
6. Bogdandy Von, A., Nettesheim, M. (1996). *Ex Pluribus Unum: Fusion of the European Communities into the European Union*. European Law Journal, Nr. 2/3, 267-289.
7. Craig, P., de Burca, G. (2020). *EU Law, Text, Cases and Materials*, Oxford University Press, seventh Edition.
8. Chander, A. (2020). *Is Data Localisation a Solution for Schrems II*, Journal of International Economic Law, Georgertown University Law Center.
9. Cuirtin, D. (1993). *The constitutional structure of the Union: a Europe of bits and pieces*. Common Market Law Review, 17.
10. Curtin, D. / Meijers, H. (1995). *The Principles of Open Government in Schengen and the European Union: Democratic Retrogression?* 32 Common Market Law Review, 391-441.
11. Duić, D. (2019). *Migracijsko pravo EU-a i prava djeteta // Prekogranično kretanje djece u Europskoj uniji* / Župan, Mirela (ur.). Osijek: Pravni fakultet Osijek, 131-155.
12. Đurđević, Z. (2008). *Lisabonski ugovor – prekretnica u razvoju kaznenog prava u Europi*. Hrvatski ljetopis za kazneno pravo i praksu, 15 (2), 1077-1127.
13. Editorial comment (1995). *Schengen: The pros and cons.* Common Market Law Review 32, 673-678.
14. Glouftsios, G., Bellanova, R. (2020). *Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintanance*. Geopolitics, 1-21.
15. Groussot, X. *General Principles of Community Law*. Europa Law Publishing, Groningen, 2006.
16. Guild, E. (2007). Inquiry into the EU-US Passenger Name Record Agreement. CEPS Policy Brief, No. 125.
17. Hailbronner, K./Thierry, C. (1997). *Schengen II and Dublin, Responsibility for Asylum Applications in Europe*. 34 Common Market Law Review, 957–989.
18. Heukels, T., Blokker, N., Brus, M. (ur), (1998). The European Union after Amsterdam – A Legal Analysis. Kluwer; The Hague. 51-68.

19. Jokhadze, N. (2020). *Implementation of Interoperability of EU Information Systems in the Justice and Home Affairs domain. Challenges and Opportunities*, School of Business and Governance, Talinn University of Technology (Mater's thesis, supervisor Dr. Aleksands Cepilovs).
20. Jeandesboz, J., Bigo, D., Hayes, B. & Simon, S. (2013). *The Commission's legislative proposals on Smart Borders: their feasibility and costs*. European Parliament, p. 1-67.
21. Leidenmuhler, F. (2002). The incorporation of the Schengen acquis into the framework of the EZ by example of the „ne bi in idem" principle. The European Legal Forum, 5, p. 253-275.
22. Meijer, H., Bolten, J. et al. (eds). *Schengen. Internationalisation of Central Chapters of the Law of Aliens, Refugees, Privacy, Security, and the Police*. Antwerp: Kluwer, 5-6.
23. Muller-Graff, P. (1994). The legal bases of the third pillar and its position in the framework of the Union. Treaty'. Common Market Law Review, 493.
24. Nanz, K.P. (1995). *The Schengen Agreement: Preparing the Free Movement of Persons in the European Union*. in Bieber, R./Monar, J. (eds. 1995). Justice and Home Affairs in the European Union. The Development of the Third Pillar, Brussels, 29-48.
25. Napieralski, A. (2019). *Collecting Data at EU Smart Borders: Data Protection Challenges of the New Entry/Exit System*. Juridikum. Zeitschrift für Kritik, Recht, Gesellschaft vol. 2, p. 200-210.
26. O'Keeffe, D. (1991). *The Schengen Convention: A Suitable Model for European Integration?,* Yearbook of European Law, 185-219.
27. Oliveira, A.A.Y. (2019). *Recent Developments of interoperability in the EU area of Freedom, Security and Justice: Regulations* (EU) 2019/818 and 2019/818. UNIO-EU Law Journal, Vol. 5, No.2, p. 128-135.
28. Pejaković- Đipić, S., Karas, Ž. (2018). *Neki problemi kod prikupljanja i razmjene podataka o putnicima u zračnom prometu*. Policija i sigurnost, 27 (4), 435-457.
29. Peers, S. (2011). *EU Justice and Home Affairs Law (non-civil). "The Evolution of EU Law.* Oxford University Press.
30. Petrašević, T., Duić, D. (2016). *Direktiva o evidenciji podataka o putnicima (PNR) i zaštita podataka u EU*. Zbornik radova 5. Međunarodne znanstveno-stručne konferencije „Unaprjeđivanje sigurnosne uloge policije primjenom novih tehnologija i metoda" / Vukosav, Joško; Butorac, Ksenija; Sindik, Joško (ur.), Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija, 638-652.
31. Quintel, T. (2018). *Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention.* University of Luxembourg Law Working Paper No. 002-2018, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3132506 – accessed on 17 October 2021).
32. Rijpma, J. J. (2009). *EU Border Management After the Lisbon Treaty*. Croatian Yearbook of European Law and Policy, 5, p. 93-121.
33. Roots, L. (2015). *The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination' Baltic Journal of European Studies*, Vol. 5, No. 2, pp. 108-129.
34. Rošić, M. (2014). *Najznačajniji aspekti međunarodne policijske suradnje Republike Hrvatske s državama* članicama *Europske unije* (The Most Significant Aspects of International Police Cooperation of the Republic of Croatia with the EU Member States). Hrvatski ljetopis za kazneno pravo i praksu. 21(2), 295-326.
35. Schutte, Julian J. E. (1991). *Schengen: it's meaning for the free movement of person in Europe*. Common Market Law Review 28, 549-570.
36. Schutte, J.J.E. (1993). *The European Market of 1993*. 3 Criminal Law Forum, 55-83.

37. Steffens, F. (2020). Facing up to the New World of Border Control, Biometric Technology Today, Issue 9, p. 8-11.
38. Tridimas, T. (2006). *The general principles of EU law*. Oxford University Press, 2006.
39. Vedaschi, A. (2018). *The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017, Opinion 1/15*. European Constitutional Law Review, Vol. 14 No. 2: 410-429.
40. Woltjer, A. (1995). *Schengen: The Way of No Return?,* 2nd Maastricht Journal, 256-278.
41. Wessel, R. (2000). *The Inside Looking Out: Consistency and Delimitation in EU External Relations*. Common Market Law Review, 37/5, 1135-1171.
42. Wagner, E. (1998). The Integration of Schengen into the Framework of the European Union. Legal Issues of Economic Integration, 25(2), p. 1-60.

Official documents

1. Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders; Official Journal L 239 , 22/09/2000 P. 0013–0018.
2. Commission Decision of 17 June 2016 setting up the high – level expert group on information systems and interoperability – 2016/C 257/03.
3. Eurodac – 2017 statistics'. February 2018. https://www.eulisa.europa.eu/Publications/Reports/Eurodac%20Statistics%202017.pdf (Accessed 24 July 2019)
4. European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission work Programme 2017.
5. European Commission: Seventh progress report towards an effective and genuine Security Union.
6. European Commission (EC): Communication Stronger and smarter information borders and security.
7. European Commission (2010) Staff Working Document on the fulfilment of the 29 measures for reinforcing the protection of the external borders and combating illegal immigration adopted at the Justice and Home Affairs Council meeting, held on Brussels on 25 and 26 February 2010. Brussels, SEC (2010) 1480 final, 26.11.2010.
8. European Commission (2008) Preparing the next steps in border management in the European Union - Impact Assessment. Brussels, SEC (2008) 153 final, 13.2.2008.
9. European Policy Evaluation Consortium (2004) Study for the extended impact assessment of Visa Information System. Brussels, December 2004.
10. FRA (2018) 'Interoperability and Human Rights Implications: Opinion of the European Union Agency for Fundamental Rights'. FRA Opinion – 1/2018 [Interoperability], 19 April 2018. http://fra.europa.eu/en/opinion/2018/interoperability (accessed 29 January 2019).
11. Roadmap of June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area – 9368/1/16 REV 1.

EU Legislation

1. Consolidated version of the Treaty on the Functioning of the European Union (2012), OJ C326/47.
2. Council Regulations (EC) No 1683/95 and (EC) No 539/2001 and Regulations (EC) 32 No 767/2008 and (EC) No 810/2009 of the European Parliament and of the Council. OJ L 182/1.
3. Directive (EU) No. 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L119/89.
4. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L119/132.
5. Explanatory Memorandum of the Proposal for the EES Regulation COM/2016/0194 final - 2016/0106 (COD).
6. Protocol (No 2) integrating the Schengen acquis into the framework of the European Union (OJ 1997 C 340, at 93).
7. Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December, 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II). OJ L 381/4.
8. Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). OJ L 218/60.
9. Regulation (EU) No. 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. OJ L 286/1.
10. Regulation (EU) No 610/2013 of the European Parliament and of the Council of 26 June 2013 amending Regulation (EC) No 562/2006 of the European Parliament and of the Council establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), the Convention implementing the Schengen Agreement.
11. Regulation (EU) No. 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L77/1.
12. Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1.
13. Regulation (EU) No. 2017/2226 of the European Parliament and of the Council 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.
14. Regulation (EU) No. 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System

(ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226. OJ L 236/1.

15. Regulation (EU) No. 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726. OJ L 135/1.
16. Regulation (EU) No. 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 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA. OJ L135/27.
17. Regulation (EU) 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. OJ L135/85.
18. Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System [2021] OJ L248/1.
19. Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System [2021] OJ L248/11.
20. The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, [2000] OJ L 239.

Judgments of the European Court

1. Case C-120/94 *Commission of the European Communities v Hellenic Republic*, [1996], ECLI:EU:C:1996:116, Opinion of Advocate General Jacobs.
2. Case C-101/01 *Criminal proceedings against Bodil Lindqvist*, (2003) ECR, I-12971.
3. Case C-105/03, *Pupino* (ECJ 16 June 2005).
4. Case C-176/03, *Commission v. Council* (ECJ 13 September 2005).
5. Cases C-317/04 and C-318/04, *Parliament v. Council and Commission* (ECJ 30 May 2006).
6. Case C-440/05, *Commission v. Council*,(ECJ 23 October 2007).
7. Case C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* (2008) ECR I-00271
8. Case C-301/06, *Ireland v. Council and Parliament* (ECJ 10 February 2009).
9. Case C-482/08, *UK v. Council* (ECJ 26 October 2010).

10. Opinion 1/15 (Passenger name record data (European Union/Canada) ECLI:EU:C:2016:656.
11. Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (2020) ECLI:EU:C:2020:559

List of Abbreviations:

1. ABC gates: Automated Border Control
2. AFSJ: Area of Freedom, Security and Justice
3. CIR: common identity repository
4. CFSP: Common Foreign and Security Policy
5. COMM: European Commission
6. CRRS: Central Repository for reporting and Statistics
7. EC: European Community
8. ECRIS – TCN: European Criminal Records Information System for Third Country Nationals
9. EDPS: European Data Protection Supervisor
10. EES: Entry – Exit system
11. EP: European Parliament
12. ESP: European search portal
13. ESTA: Electoral System of Travel Authorization
14. ETIAS: European Travel Information and Authorisation System
15. EU VIS: Visa Information System
16. HLEG: High-level Expert Group on information systems and interoperability
17. JHA: Justice and Home Affairs
18. MID: multiple identity detector
19. PNR: Passenger Name Record
20. RTP: Registered Traveller Program
21. Schrems II case: Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems
22. sBMS: shared biometric matching service
23. SIS: Schengen Information System
24. TEC: Treaty of Amsterdam
25. TFEU: Treaty on the Functioning of the EU
26. US: United States

Sažetak

Dunja Duić, Marijo Rošić

Interoperabilnost EU sustava - od ideje do realizacije

Ovaj članak daje pregled nastanka interoperabilnosti EU sustava čiji je glavni cilj spajanje šest EU zbirki podataka u jedinstven sustav kojim će se pospješiti opće stanje sigurnosti EU-a i suzbiti nezakonite migracije. U prvome dijelu članka detaljno je opisan pravni okvir koji je prethodio uspostavi interoperabilnosti EU informacijskih sustava i pojašnjeni su razlozi uspostave. Članak opisuje svrhu svakoga pojedinog sustava i njihovu međuzavisnost, uzajamnu povezanost i praktično djelovanje. Na temelju te međuzavisnosti, u članku se nadalje opisuju pojedini scenariji praktične primjene i moguće implikacije na rad tijela kaznenog progona u EU-u. Autori pojašnjavaju sličnosti primjene PNR sustava i interoperabilnosti. Analizom raspoložive sudske prakse u primjeni PNR-a, autori analiziraju moguće sudske posljedice primjene načela proporcionalnosti u budućoj praktičnoj provedbi interoperabilnosti. Dodatno, kroz analize budućih scenarija praktične provedbe interoperabilnosti, članak ukazuje na moguće provedbene i zakonodavne nedostatke. Rad se zasniva na komparativnoj, povijesnoj metodi i analizi slučajeva.

Ključne riječi: interoperabilnost, proporcionalnost, PNR, SIS, VIS, EES, ETIAS, Eurodac, ECRIS-TCN.