the SPANISH YEARBOOK of INTERNATIONAL LAW

The Interoperability of EU Information Systems and Fundamental Rights concerns

Elisabeth HOFFBERGER-PIPPAN*

Abstract: In early 2019, the Council of the European Union, together with the Parliament, adopted Regulation 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders, visa and law enforcement. This is the first legislative act ever adopted creating such a large-scale interoperable framework. Until recently, the different EU information systems were strictly separated, fragmented and disconnected. By establishing interoperability, national authorities are now able to access data on the identity of persons fast and easy without major bureaucratic or administrative hurdles. By establishing such a framework it is now possible to better prevent potential terrorist threats and migration-related crimes, such as human trafficking. At the same time it gets more and more obvious that individuals, especially third-country nationals, are increasingly becoming transparent. While the prevention of terrorism and the maintenance or re-establishment of internal security clearly constitute legitimate interests of society, establishing interoperability between EU information systems raises fundamental rights concerns, especially with regard to data protection and the right to privacy. When the European Commission adopted its final proposal for the aforementioned regulation in 2018, the Fundamental Rights Agency (FRA) was asked to evaluate the text with regard to potential fundamental rights violations. Furthermore, the European Data Protection Supervisor (EDPS) and the Data Protection Working Party (WP29) analyzed the proposal from a legal perspective and scrutinized it carefully. It turned out that especially the law on data protection, as well as the case law provided by the ECJ had significant impact on Regulation 2019/817 and the way in which it had been finally formulated. Overall, the criticism expressed by the FRA, the EDPS and the WP29 has been taken seriously by the Council and the Parliament respectively. Nevertheless, account shall be taken of the fact that a general trend within the EU can be observed of granting authorities access to different systems and databases which were originally established for different purposes. This development makes it all the more important to be particularly cautious when it comes to adopting and formulating EU legislation.

Keywords: data protection interoperability EU information systems right to private life fundamental rights data minimisation purpose limitation

(A) INTRODUCTION

Since 2015, the European Union (EU) has been facing an unprecedented wave of migrants and refugees. The rising number of people trying to enter the EU through either the so-called "Balkan Route" or the Mediterranean Sea has jeopardized and caused the lives of many people, including children. At the same time, EU Member States have been increasingly overwhelmed with the situation especially by the great number of "irregular arrivals", which resulted *inter alia* in the tightening of rules for asylum seekers and migrants. The number of people trying to enter the EU dropped significantly within the last two years but considering the continuous political tensions worldwide and other factors, such as climate change, more people are expected to arrive in the coming years.[1]

The large influx of third-country nationals challenged (and is still challenging) the EU and its Member States in a twofold manner. On the one hand, thousands of people risk their lives when fleeing or migrating to Europe, for example when crossing the Mediterranean Sea trying to reach European shores. Many are

Article published on 31 December 2019

* Senior Researcher, Johannes Kepler University Linz. Mail: Elisabeth.Hoffberger@jku.at.

[1] Eurostat, Asylum Statistics, text available electronically at https://ec.europa.eu/eurostat/statistics-explained/index.php/Asylum_statistics, accessed 31 July 2019.

 DOI: 10.17103/sybil.23.4

stranded in camps living in constant fear of deportation. On the other hand, the rising number of "irregular arrivals" has given rise to security concerns in EU Member States. In early 2015, the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, called upon the UN-Security Council to support efforts of the EU to combat the trafficking in migrants and similar criminal offences.[2] After it had turned out that at least one of the terrorists who killed more than 120 people in the 2015 Paris terror attacks supposedly was a Syrian refugee who had entered Europe via Greece, security issues with regard to the so-called "refugee and migratory crisis" became the center of the political debate in Europe.[3]

The EU has already provided for an abundance of instruments and measures in order to regulate and control the entry of third-country nationals and to handle security concerns in general by enacting legislation on border management and law enforcement. These measures include *inter alia* the establishment of the Schengen Information System[4] (SIS), as well as the Visa Information System[5] (VIS) and the adoption of the Eurodac Regulation[6]. All these systems collect different types of personal data, reaching from fingerprints to facial images and in some cases DNA. Until recently, these systems were fragmented, strictly separated and unconnected.[7] In order to respond better to the aforementioned challenges, the European Commission (EC) – on the invitation of the Council[8] – adopted its first proposal for a Regulation on establishing a framework for interoperability between EU information systems in

[2] The Telegraph, 'Migrant Crisis is a Security Crisis' says EU Foreign Policy Chief, accessed 31 July 2019.

[3] CNN, Passport Linked to Terrorist Complicates Syrian Refugee Crisis, accessed 31 July 2019.

[4] Regulation 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 2006 L 381/4; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ 2007 L 205/63; Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, OJ 2006 L 381/1.

[5] Council Decision 2004/12/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ 2004 L 213/5; Regulation 767/2008 of the European Parliament and of the Council of July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ 2008 L 218/60.

[6] Regulation 603/2013 of the European Parliament and of the Council of 26 June 2013 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 and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ 2013 L 180/1.

[7] Cf. Amended Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation], 13 June 2018, COM/2018/478 final.

[8] Draft Council Statement calling on the Commission to Propose a Comprehensive Framework for Law Enforcement Access to Various Databases in the Area of Justice and Home Affairs, with a View to Greater Simplification, Consistency, Effectiveness an Attention to Operational Needs, Summary Record of 21 March 2017, 7177/18.

 DOI: 10.17103/sybil.23.4

2017.[9] After lengthy discussions within the Council,[10] the Commission adopted and amended the proposal in 2018.[11] After having consulted the FRA[12], the EDPS[13] as well as WP29[14], the Council together with the Parliament adopted Regulation 2019/817. Apparently, the Council and the Parliament took the criticism expressed by the aforementioned institutions seriously, as Regulation 2019/817 deviates clearly from the Commission's original proposal.

This article aims to analyze the significant influence the FRA, the EDPS and the WP29 played in the process of adopting Regulation 2019/817. The breaking down of immaterial walls by establishing interoperability and thus making individuals more transparent is as such clearly opposed to the distinct fundamental rights awareness within the EU. The FRA, the EDPS as well as the WP29 contributed to the process of adopting Regulation 2019/817 greatly and at the same time the Council and the Parliament have worked together with these three institutions on a constructive basis. Admittedly, weighing between legitimate interests of society as a whole, such as the prevention of terrorist threats and fundamental rights protection is a true balancing act. Regulation 2019/817 seems to have found that balance. Given the significant complexity of Regulation 2019/817, it cannot be ruled out that the ECJ will soon be called upon to clarify certain elements of it, for example by way of preliminary rulings procedure. For the time being, however, the Regulation can be summarised as a positive step forward in order to face current challenges adequately, while at the same time making sure that fundamental rights are sufficiently protected.

---

9 Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM/2017/0793 final.

10 See, for example, Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, ST 15119 2017 INIT. For more details see Procedure 2017/0351/COD, electronically available at https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2017:0793:FIN/2017-12-14_DIS_byCONSIL, accessed 31 July 2019.

11 Amended Proposal COM/2018/478 final, *supra* n. 7.

12 FRA, Interoperability and fundamental rights implications, Opinion of the European Union Agency for Fundamental Rights, 11 April 2018, FRA Opinion 1/2018; Regulation (EU) 2019/817 of the European Parliament and 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 2019 L 135/27. See also M. Gutheil, Q. Liger, J. Eager, Yemi Oviosu and D. Bogdanovic, *Interoperability of Justice and Home Affairs Information Systems*, Study for the Libe Committee, April 2018, PE 604.947; P. Hanke/D. Vitello, *High-Tech Migration Control in the EU and Beyond: The Legal Challenges of "Enhanced Interoperability"* in E. Carpanelli/N. Lazzerini (eds.), *Use and Misuse of New Technologies* (Springer, Cham 2019) at 3–35.

13 EDPS, Opinion 4/2018 on the Proposals for two Regulations establishing a framework for the interoperability between EU large-scale information systems, 16 April 2018. See also Summary of the Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 4 July 2018, C 233/12. See also the Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017.

14 WP29, Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration, 11 April 2018, WP266, 18/EN. In this context, processes which have taken place at the level of the Council of Europe should be mentioned as well. See, for example, the Practical guide on the use of personal data in the police sector, 15 February 2018, T-PD(2018)01.

(B) CURRENT AND FUTURE IT SYSTEMS

Regulation 2019/817 foresees that the Schengen Information System (SIS)[15], the Visa Information System (VIS)[16] and the Eurodac Regulation[17] will be made interoperable in order to facilitate border management and law enforcement by reducing administrative and technical hurdles and to guarantee better and faster access to different kinds of data. Furthermore, three new IT systems will supplement the pre-existent ones, namely the Entry-Exit System (EES)[18], the European Travel Information and Authorisation System (ETIAS)[19] as well as the European Criminal Record Information System for third-country nationals (ECRIS-TCN)[20]. In addition, Regulation 2019/817 includes the Stolen and Lost Travel Documents Database (SLTD)[21] provided by Interpol.[22] It also entails data provided by Europol[23] in as much as it is

15 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 2006 L 381/4; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ 2007 L 205/63; Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, OJ 2006 L 381/1. On the latest developments regarding the SIS see Council of the European Union, Press Releases, Schengen Information System: Council adopts new rules to strengthen security in the EU, accessed 31 July 2019.

16 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 2008 L 218/60.

17 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 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 and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ 2013 L 180/1.

18 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 2017 L 327/20.

19 Regulation (EU) 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 2018 L 236/1.

20 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 nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ 2019 L 135/1.

21 Interpol, Stolen and Lost Travel Documents database, accessed 31 July 2019.

22 Cf. Amended Proposal, COM/2018/478 final, *supra* n. 7, Explanatory Memorandum.

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

 DOI: 10.17103/sybil.23.4

relevant for the ETIAS. The Prüm Framework[24], the Passenger Name Record Directive (PNRD)[25] as well as the Advance Passenger Information Directive (APID)[26] are not part of the Regulation.[27]

(1) The Schengen Information System (SIS)

The SIS was the first EU-wide IT system in the area of border management and law enforcement.[28] With the entry into force of the Schengen Convention in 1995 it finally became operative.[29] The SIS allows Member States authorities to consult and enter alerts on both persons and objects. In 2013, the original SIS was replaced by SIS II,[30] a more advanced version of the SIS with more competences and functionalities, such as the use of biometric data, the possibility of linking alerts, as well as the competence to store copies of the European Arrest Warrant (EAW).[31] Given the fact that the SIS II was endowed with such a broad range of competences, ranging from immigration policy to police and judicial cooperation, it is based on three different legislative acts.[32] Regulation 1987/2006[33] addresses the area of border management by allowing border guards, visa issuing as well as migration authorities "to enter an alert or consult alerts on third-country nationals for the purpose of refusing their entry into or stay in the Schengen area."[34] Council Decision 2007/533/JHA[35] allows both police as well as judicial cooperation with regard to missing persons and persons or objects in connection with criminal offences, including persons wanted for arrest or for surrender purposes. Furthermore, Regulation No. 1986/2006[36] establishes an alert system for stolen vehicles. Currently, thirty different countries are participating at the SIS II, including 26 EU Member States and 4 Schengen Associated Countries (Iceland, Liechtenstein, Norway and Switzerland).

---

[24] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008 L 210.

[25] 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 2016 L 119.

[26] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ 2004 L 261.

[27] Amended Proposal COM/2018/478 final, *supra* n. 7, Explanatory Memorandum.

[28] Cf. F. Boehm, *Information Sharing Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level* (Springer, Berlin – Heidelberg 2012), at 260.

[29] *Ibid.* Convention Implementing the Schengen Agreement of 14 June 1985, 22 September 2000, OJ L 239.

[30] Originally, it was planned to replace the SIS in 2007. Due to technical problems, the SIS II could be finally realized in 2013.

[31] European Commission, Migration and Home Affairs, Second generation Schengen Information System (SIS II), accessed 31 July 2019.

[32] Cf. F. Boehm, *Information Sharing*, *supra* n. 28, at 262.

[33] 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), 28 December 2006, OJ L 381.

[34] See European Commission, Migration and Home Affairs, Schengen Information System, accessed 31 July 2019.

[35] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), 7 August 2007, OJ L 205.

[36] Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, 28 December 2012, L 381/1.

 DOI: 10.17103/sybil.23.4

Ireland and Cyprus do not participate at the SIS itself, while the UK operates the SIS without participating at the Schengen area.[37] In 2018, the Council and the Parliament reached an agreement to broaden the types of biometric data which can be stored in the SIS, which will also include DNA.[38]

(2) The VISA Information System (VIS)

The VIS, which was established by Council Decision 2004/512,[39] allows Schengen states to exchange visa data.[40] It consists of a central information system and a communication infrastructure between the central information system and its national counterpart in the EU Member States.[41] After lengthy discussions, an updated version of the VIS was adopted in 2008 with the entry into force of the VIS Regulation[42] allowing for the first time to store biometric data. When applying for a visa, applicants leave their fingerprints as well as a photograph. Using biometric data helps clarify whether a person is the rightful holder of his/her identity documents. The VIS was created for the purpose of *inter alia* facilitating visa procedures, to fight against fraud and most of all to prevent threats against the internal security of EU Member States. According to the VIS Regulation, visa applications are stored irrespective of whether a visa had been issued, annulled, extended, revoked or refused.[43] The gathered data reach from "short-stay visas to transit visas, airport transit visas, visas with limited territorial validity and long stay visas".[44]

(3) The Eurodac Regulation

Eurodac[45] can be described as a fingerprint database for asylum procedures. Whenever an individual applies for asylum, his/her fingerprints are taken and transferred to the Eurodac database. The Eurodac system was created to implement the Dublin II Regulation[46], which aims to ascertain which country is responsible for the examination of an asylum application.[47] The first Eurodac Regulation was adopted in

37 For more details, see Schengen Information System, European Commission, accessed 31 July 2019.

38 *Ibid.*

39 Council Decision of 8 June 2004 establishing the Visa Information System (VIS), (2004/512/EC), OJ 2004 L 213/5.

40 F. Boehm, *Information Sharing*, *supra* n. 28, at 281.

41 Council Decision 2004/512/EC, *supra* n. 39, Art 1 para 2.

42 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 2008 L 218/60.

43 *Ibid.* Art 10 – 14. Cf. F. Boehm, *Information Sharing supra* n. 28, at 280 – 281.

44 *Ibid.* 283.

45 Regulation 603/2013, *supra* 6.

46 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, replaced by Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 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, OJ 2013 L 180/31.

47 Cf. F. Boehm, *Information Sharing*, *supra* n. 28, at 304 – 305.

 DOI: 10.17103/sybil.23.4

2000[48], whereas the system as such had been operatively active since 2003.[49] National asylum authorities may enter the Eurodac system and find out whether the applicant has already applied for asylum in a different EU country.[50] In addition, police authorities are also allowed to consult the Eurodac system under very narrow circumstances.[51] In general, the Eurodac database contains all different kinds of data, including *inter alia* fingerprints of asylum seekers but also of migrants, who have been arrested for crossing illegally EU borders. Furthermore, the Eurodac Regulation allows to take fingerprints of those persons, who have been found illegally in one of the EU's Member States.[52]

(4) The Entry-Exit System (EES) and the European Travel Information and Authorisation System (ETIAS)

The Entry-Exist System[53] is a new system that will collect data of visa-required as well as visa-exempt third-country nationals, who are permitted to stay in the Schengen area with a short-term visa (90 days).[54] It replaces the manual stamping of passports and allows for the storage of different types of data, including biometrics.[55] The system is able to evaluate the exact moment a short-term visa expires and the exact point of time an individual has no legal status to reside in the EU anymore.[56] It is the overall purpose of the EES, to "improve the management of external borders, to prevent irregular immigration and to facilitate the management of migration flows."[57] Eu-LISA will be responsible for the technical feasibility of the EES, which will be operable as from 2020.[58]

The European Travel Information and Authorisation System (ETIAS)[59] is an electronic travel authorisation system comparable to the US-American model "ESTA". It applies to third-country nationals coming from visa-exempt countries wishing to enter the Schengen area. They will have to undergo

48 Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ 2000 L 316.

49 Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 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, OJ 2013 L 180.

50 T. Balzacq/S. Carrera, *Migration, Borders and Asylum: Trends and Vulnerabilities in EU Policy* (Centre for European Policy Studies, Brussels 2005) 45.

51 Regulation 603/2013, *supra* n. 6.

52 For more information see Boehm, *Information Sharing*, *supra* n. 28, at 306.

53 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 2017 L 327.

54 *Ibid.* Art 16 and 17.

55 Cf. *Ibid.* Art 17.

56 Cf. European Council, Entry-exit system: final adoption by the Council, accessed 31 July 2019.

57 Regulation 2017/2226, *supra* n. 53, recital 15.

58 European Council, Entry-exit system: final adoption by the Council, *supra* n. 56.

59 Regulation (EU) 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 2018 L 236.

additional security checks and to pay a fee prior to their entry into the Schengen area.[60] It is expected that ETIAS will be operational in 2020.[61]

(5) The European Criminal Record Information System (ECRIS-TCN)

The European Criminal Record Information System for third-country nationals (ECRIS-TCN system) is an electronic system processing personal data of third-country nationals as well as stateless persons within the EU, who have been convicted of a crime and whose conviction is stored in the Member States' criminal records. [62] Collected data encompass both alphanumeric data and fingerprints. Under certain circumstances, the storage of facial images shall be possible as well.[63] The ECRIS-TCN is part of a greater "ECRIS" package,[64] which seeks to collect data on both EU citizens and third-country nationals as well as stateless persons, who have been convicted of a criminal offence and whose conviction appears in one of the criminal records databases.[65] While the former ECRIS system worked on a decentralised basis, the new ECRIS-TCN will be a centralized system allowing Member States to ascertain which EU country holds criminal records about a third-country national or a stateless person.[66] The ECRIS-TCN will be operable within the next years.[67]

(C) REGULATION 2019/817

Regulation 2019/817 aims to create the interoperability of the aforementioned systems, which are either already existing or which will be operatively active soon. In order to do so, the Commission is planning to create four different mechanisms, which will be elaborated in more detail in the following chapter.

(1) The European Search Portal (ESP)

The ESP will function as a "message broker" allowing for the simultaneous querying in different IT systems, such as the VIS, Eurodac, EES etc. It is the overall aim to guarantee "fast, seamless, efficient, systematic and controlled access by Member State authorities and Union agencies to the EU information systems, Europol systems and Interpol databases".[68] However, national authorities shall only have access

---

60 *Ibid.* Art 1.

61 ETIAS Homepage, accessed 31 July 2019.

62 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 nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ 2019 L 135/1.

63 *Ibid.* Recital 15.

64 *Ibid.* See also Directive (EU) 2019/884 of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, OJ 2019 L 151/143.

65 European Commission, EU Information Systems, Security and Borders, accessed 31 July 2019.

66 Regulation 2019/817, *supra* n. 12, Art 5 – 8.

67 European Commission, EU Information Systems, Security and Borders, *supra* n. 65.

68 Regulation 2019/817, *supra* n. 12, recital 13.

 DOI: 10.17103/sybil.23.4

to those databases they are allowed to access according to their relevant (national) access rights.[69] As already indicated, the ESP will be used to query simultaneously the EES, the VIS, ETIAS, Eurodac and ECRIS-TCN but it will also be an additional tool to query the SIS, Interpol and Europol by "complementing the existing dedicated interfaces."[70] The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Eu-LISA) will develop the ESP and guarantee its technical feasibility.[71] In order to specify the technical details of the relevant system, the Commission is authorized to adopt delegated acts.[72] Logs will be kept of all processed data including the information on which national authority entered the query as well as the time and the date of the query. The data will be deleted one year after they had been established.[73]

(2) The Biometric Matching Service (BMS)

The BMS will supplement the CIR, the MID as well as the EES, the VIS, the Eurodac and the SIS. Instead of entering queries based on the name of a specific person, biometric data can be used to enter a query by storing so-called biometric templates.[74] It will consist of a centralized infrastructure which will store all different types of biometric data, including data stored in the EES, the VIS, the SIS, the Eurodac system as well as the ECRIS-TCN.[75] Regulation 2019/87 emphasizes that Member States have to guarantee minimum standards of data quality when entering data into the aforementioned systems. As in the case of the ESP, logs will be kept containing information on the creation of the biometric templates, information on which EU information system had been queried by the BMS, the type of biometric data, date, time of the relevant query as well as its length. One year after their creation, the logs shall be erased.[76] Regulation 2019/87 also refers to questions relating to data retention. According to the Regulation, the data stored in the BMS shall be stored as long as they are stored in the underlying systems, that is to say, in the CIR or the SIS.[77]

---

69 *Ibid.* Art 6 para 1.

70 *Ibid.* Recital 17. It is worthy of note that the SIS, Europol and Interpol already have centralized systems as well as national systems and a communication infrastructure between the national and the centralized systems. See, for example, 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 2006 L 381/4. Art 4. Therefore, the ESP will be an additional tool to query these systems. Whether this may change in future remains to be seen.

71 *Ibid.* Art 6 para 3.

72 *Ibid.* Art 9 para 7.

73 *Ibid.* Art 10. For more details see Bogensberger, *Police Cooperation* in: M. Klamert/M. Kellerbauer/J. Tomkin, Commentary on the EU: Treaties and the Charter of Fundamental Rights (Oxford University Press, Oxford 2019) 925 – 938, at 930.

74 Regulation (EC) No. 1987/2006, *supra* n. 70, Art 12 para 1 and Art 14.

75 *Ibid.* Art 13.

76 *Ibid.* Art 16 para 2.

77 *Ibid.* Art 15. Cf. Bogensberger, *Police Cooperation*, *supra* n. 73, at 930. See also P. de Hert/J. Saifert, Police, Privacy and Data Protection from A Comparative Legal Perspective, in: M. den Boer (ed.), Comparative Policing from a Legal Perspective (Edward Elgar Publishing, Cheltenham – Northampton 2018) 306 – 328, at 332.

 DOI: 10.17103/sybil.23.4

(3) The Common Identity Repository (CIR)

The CIR will create an individual file of each person whose information is contained in the EES, the VIS, the Eurodac, the ECRIS-TCN and ETIAS. It will allow *inter alia* police authorities – in accordance with their powers under national law – to access the CIR which contains biometric data of a person. Member States authorities will be able to access the CIR for different purposes. Where the national law allows so, police authorities may query the CIR solely for the purpose of identifying a person.[78] This might include biometric data, such as fingerprints. In addition, whenever it turns out that a person might be having multiple identities,[79] the Member States authorities may query the CIR and access all the information contained therein. Likewise, Member States authorities may query the CIR in order to prevent, detect or investigate into possible terror acts or other, serious criminal offences. Whenever it turns out that data on a person are contained in the CIR, the CIR replies by making a reference indicating which of the aforementioned systems contains such information (hit/no-hit).[80] In order to be granted full access to the data contained therein, the Member States themselves can authorize their national authorities in this regard.[81] As in the case of the BMS, data contained in the CIR will be stored and retained as long as they exist in the underlying systems. Again, logs will be kept for a maximum of one year containing information, such as the purpose of the access, the time and duration of the query as well as their result.[82]

(4) The Multiple Identity Detector (MID)

The MID primarily serves the purpose of storing links between data contained in the relevant information systems, such as the CIR (which covers the data contained in the VIS, ETIAS, Eurodac and the ECRIS-TCN system) and the SIS. It is the overall aim to facilitate identity checks in general and to detect possible identity fraud.[83] The launching of a multiple detection might be necessary in case an individual file is created according to the EES regulation, in case an application file is provided according to the VIS, the ETIAS regulation or an alert entered into the SIS. The whole system works on a hit/no-hit basis. In case the system reveals that both the biometrical as well as the identity data are identical, a white link is created.[84] The same holds true in case the system reveals the same biometric but different identity data but the responsible authority concludes – by manual verification – that the identify lawfully belongs to one person. In case the query reports differences, such as same biometric data but different information on identity (such as the last name), a yellow link occurs in case manual verification did not take place.[85] In case of same biometrics but similar identities, a green link occurs provided that the competent authority responsible

78 *Ibid.* Art 20.

79 Cf. *Ibid.* Art 28 para 4.

80 In this regard it should be noted that "hit flags" constitute personal data in itself and therefore require authorities to maintain sufficient procedural safeguards. See WP29, Opinion on Commission proposals, *supra* n. 14, at 21.

81 *Ibid.* Art 22. Cf. Bogensberger, *Police Cooperation*, *supra* n. 73, at 930.

82 *Ibid.* Art 24.

83 *Ibid.* Art 25.

84 *Ibid.* Art 33.

85 *Ibid.* Art 30.

 DOI: 10.17103/sybil.23.4

with regard to the relevant subject matter concludes that the different data on identity belong to different persons.[86] A red link occurs in case the data reveals same biometric but different data on a person's identity and the relevant national authority arrives at the conclusion that the different identities unlawfully belong to one person only.[87]

As in the case of the CIR and the BMS, the MID will retain the relevant information as long as it is stored in the underlying systems. Logs will be kept containing information on the purpose of access, the exact date and duration of the query as well as the reference to the relevant data linked.[88]

(D) FUNDAMENTAL RIGHTS CONCERNS

As already mentioned, the FRA, the EDPS as well as the WP29 were asked to comment on the Commission's proposal establishing an interoperable EU information system. All three of them expressed serious concern over potential fundamental rights violations, most of all the right to data protection.[89] Apparently, the Council as well as the Parliament took the criticism seriously when finally adopting Regulation 2019/817. In fact, the final Regulation deviates clearly from the Commission's original proposal of 2018.

According to its "founding document", Council Regulation 168/2007, the FRA is allowed to refer to a plethora of legal sources including the Fundamental Rights Charter (FRC)[90], EU secondary law and the European Convention on Human Rights (ECHR)[91]. However, in its 2018 opinion, the agency addressed the ECHR only marginally, while primarily focussing on the FRC as well as EU secondary law.[92] In substantial terms it is worthy of note that the FRA primarily scrutinized the Commission's proposal with regard to the right to non-discrimination and the right to protection of personal data. However, the FRA explicitly stressed that other fundamental rights could be jeopardized as well, such as the right to asylum, the protection on the event of removal, expulsion or extradition as well as the rights of the child and the right to an effective remedy and a fair trial.[93]

The EDPS, on the other hand, was established by Art 41 para 1 of Regulation 45/2001[94]. Its main functions include the insurance that fundamental rights and freedoms are being adhered to by the

---

86 *Ibid.* Art 31.

87 *Ibid.* Art 32. See also P. Hanke/D. Vitiello, *High Tech Migration Control in the EU and Beyond*, *supra* n. 12, at 20.

88 *Ibid.* Art 36.

89 FRA, Interoperability and Fundamental Rights Implications, *supra* n. 12. As early as in 2017, it published a report dealing with fundamental rights issues and the proposal in a more general way. See Fundamental Rights Agency, Fundamental Rights and the Interoperability of EU information systems: borders and security, 2017, accessed 31 July 2019. See also EDPS, Opinion 4/2018, *supra* n. 13, at 12; WP29, Opinion on Commission proposals, *supra* n. 14.

90 Charter of Fundamental Rights of the European Union, OJ 2012 C 326/391.

91 Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS No. 005.

92 See Council Regulation (EC) No. 168/2007 of February 2007 establishing a European Union Agency for Fundamental Rights, OJ 2007 L 53/1, recital 9 and Art 3.

93 FRA, Interoperability and Fundamental Rights Implications, *supra* n. 12, at 13 – 15.

94 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.

 DOI: 10.17103/sybil.23.4

Commission and other EU institutions.[95] At first, the EDPS acknowledged the EU's pressing need to take specific measures in the area of security and border management as especially the large influx of third-country nationals poses significant administrative but also legal challenges. According to the EDPS, the smart use of technology, for example by establishing an EU-wide information system connecting several already existing or future IT systems, is a helpful tool in accomplishing the objective of protecting and maintaining security within the EU.[96] However, the EDPS criticized the Commission's proposal for various reasons. Especially the use of data for new purposes and the facilitated identification of third-country nationals during identity checks raise severe legal concerns. Basically, the comments made by the FRA and the EDPS point in the same direction. Both institutions criticize the Commission's proposal for being – at least in some points – incompatible with the principle of purpose limitation but also with the principle of data minimisation.

The WP29 was established by Art 29 Directive 95/46/EC[97] but was replaced by the European Data Protection Board (EDPB) in 2018, which was established by Art 68 of Regulation 2016/679[98]. The criticism expressed by the WP29 is similar to the comments made by the FRA and the EDPS respectively. Especially the CIR and the principle of purpose limitation have led to concern.

This article will not analyze the criticism and comments made by the aforementioned institutions in their entirety. It is the overall purpose to analyze the broader picture and to raise awareness for the most severe and the most significant fundamental rights concerns.

(1) General Concerns: Non-Discrimination

Establishing interoperability between EU information systems may particularly affect certain groups of people, such as women and migrants, but also children, the elderly and persons with disabilities. These groups of people enjoy a multifaceted range of legal protection. While the FRC itself, with its binding nature for both the EU, its institutions and agencies, and Member States when implementing EU law, provides for an abundance of legal norms protecting vulnerable groups of people, the Commission's proposal itself contains several provisions aiming to protect those who may be particularly affected by the envisaged measures. Prior to a more in-depth legal analysis, the general fundamental rights concerns, which were especially mentioned by the FRA, seem worth mentioning.[99]

(b) *General Concerns*

95 *Ibid.* Art 41 para 2.

96 EDPS, Opinion 4/2018, *supra* n. 13, at 19.

97 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

98 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/EC (General Data Protection Regulation).

99 For more details on the competences of the EDPS see Art 46 and 47 of Regulation 45/2001, *supra* n. 94.

 DOI: 10.17103/sybil.23.4

The FRA identified the MID, which aims to tackle identity fraud as the most problematic area when it comes to fundamental rights. Whenever a query into the system results in the same biometric data but different identities, for example, the competent national authority has to ascertain whether the different identities lawfully or unlawfully belong to one or more persons. In fact, women change their identity a lot more frequently than men. In many EU countries, it is still the practice that the spouse changes her name after marriage and takes over her husbands' last name. This may increase significantly the probability that women will be stopped and scrutinized more frequently than men. Moreover, certain groups of people will also be affected negatively, especially those people coming from societies where particular names are very frequent.[100]

Another problem that will eventually arise is that the gathering of data of people with dark skin is more difficult than in the case of people with white skin as dark skin reflects less light and the quality of the data might be different.[101] Poor quality of such data may increase the risk that such people are scrutinized and checked more frequently at border crossings, for example. Children might be affected in a negative way as well.[102] Fingerprints of children may change over time significantly, especially in case fingerprints have been taken at a very young age. This may lead to "data confusion" which increases – again – the probability that children will be scrutinized and checked more often than other people. Furthermore, people with disabilities might not be able to leave fingerprints at all. If they are not provided with sufficient help and support, they will be affected more negatively by the envisaged measures than others. All these factors might – in a greater or lesser extent – amount to unlawful discrimination against vulnerable groups of people.[103]

(c) *Non-Discrimination*

The Commission's proposal aims to address the aforementioned problems. According to Art 5, the processing of personal data "shall not result in discrimination against persons on any grounds such as sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation". Taking into account that certain groups of people will be affected more negatively than others, Art 5 expressly states that "particular attention shall be paid to children, the elderly and persons with a disability".[104] However, people seeking international protection have not been qualified as vulnerable. In contrast to this, Regulation 2019/817 not only qualifies children, the elderly and the disabled as vulnerable people but also persons in need of international protection. In addition, the Regulation not only calls for the protection of the right to non-discrimination but of all other fundamental rights, including the right to private life and the right to data protection.[105]

---

[100] FRA, Interoperability and Fundamental Rights Implications, *supra* n. 12, at 13 – 15.

[101] *Ibid.*

[102] The ECtHR has expressly called upon Member States to take into account the specific needs of children also in the context of processing personal data. *S. and Marper v. The United Kingdom*, ECHR (2008), Applications Nos. 30562/04 and 30566/04, para 124.

[103] FRA, Interoperability and Fundamental Rights Implications, *supra* n. 12, at 13 – 15.

[104] Amended Proposal for a Regulation, COM/2018/478 final, *supra* n. 7, Art 5.

[105] Regulation 2019/817, *supra* n. 12, Art 5.

 DOI: 10.17103/sybil.23.4

Mentioning explicit groups of vulnerable people and requiring Member States to protect all fundamental rights is a positive sign and illustrates the Union's increased awareness for fundamental rights and their protection. However, it remains questionable whether the explicit mentioning of particular groups of people and calling upon Member States to pay particular attention to them, does have any legal repercussions. There are several arguments, which clearly support this assumption. In fact, Regulation 2019/817 is directly applicable and the terminology used in Art 5 is clear and precise, allowing individuals to derive concrete rights from it. As already indicated, people with disabilities might not be able to give their fingerprints. Member States, which do not provide sufficient support for those people, could be in violation of Art 5 of the Regulation. Likewise, children, who gave their fingerprints at a very young age and whose fingerprints changed over time, shall not face significant disadvantages by being scrutinized at borders more often than other people. The wording of Art 5 of Regulation 2019/817 obliges Member States to take specific measures in order to avoid a disproportionate burden for children, e.g. at border crossings. By the same token, the processing of data of people in need for international protection will have to be subjected to strict conditions. As the FRA criticized, it is possible that data of persons in need of international protection are being queried against Interpol databases.[106]

This entails a clear risk that information on asylum applicants becomes available to their country of origin, which could jeopardize the applicants' family members. The wording of Art 5 of Regulation 2019/817 clearly requires Member States to take active measures in order to avoid the transfer of data to non-EU countries if the processing would constitute a risk for asylum seekers or their families. The provision thus apparently takes note of the fact that particular groups of people are more likely to be affected negatively by the envisaged measures than others. By requiring Member States to pay particular attention to such people, the regulation sets an appropriately high standard of protection, which may lead to infringement proceedings before the ECJ in case of non-compliance.[107]

The WP29 criticized that Art 5 of the Commission's proposal referred to children, the elderly and people with disabilities in a rather general way, whereas other legislative acts, such as Regulation 2017/2226 establishing the Entry/Exit System refer to specific safeguards for children.[108] As a result, the WP29 concluded that the envisaged Regulation should not only entail a general clause stressing the requirement to take into account the particular vulnerability of children, the elderly and the disabled, but it should also make a clear reference to specific safeguards applied vis-à-vis these groups of people, especially in case biometric data are being processed.[109] Despite the WP29's recommendation, Regulation 2019/817 does not entail specific safeguards in this regard. The only provision taking into account the increased level of vulnerability of certain groups of people is Art 5, which – in light of the aforementioned – becomes all the more important in the context of protecting children, the elderly, the

[106] FRA, Interoperability and Fundamental Rights Implications, *supra* n. 12, at 13–15.

[107] Regulation 2019/817, *supra* n. 12, Art 5.

[108] Regulation 2017/2226, *supra* n. 18, Art 10 para 2. See also WP29, Opinion on Commission proposals, *supra* n. 14, at 17.

[109] *Ibid.*

 DOI: 10.17103/sybil.23.4

disabled and other groups of people in need of protection, which could arguably lead to infringement proceedings initiated by the Commission in case of non-compliance by Member States.

(d) *Data Quality*

Another rather technical problem especially the FRA addressed was that pictures taken from people with darker skin may be lower in quality than pictures taken from people with white skin for the sole reason that dark skin reflects less light than white skin.[110] This and other problems are realities which can only be limited by obliging Member States to establish or maintain a certain level of data quality.[111] In addition, the WP29 warned against the use of poor quality fingerprints in the BMS.[112] According to Art 13 para 3 of the Commission's proposal, biometric data shall only be entered into the system if they had undergone a quality check first. According to Art 13 para 4, the storage of data in the BMS shall meet a certain level of quality standards, which are elaborated more specifically in Art 37. Likewise, Art 18 para 3 stresses that the data stored in the CIR shall meet a certain quality standard as elaborated more specifically in Art 37, which explicitly refers to the different measures which will be taken in order to ensure data quality. Eu-LISA shall establish an automated system in order to guarantee data quality regarding data stored in the EES, ETIAS, VIS, SIS, the BMS, CIR and the MID, provide regular reports on data quality for Member States as well as the Commission itself and establish common indicators with regard to data quality. The implementation of the different quality standards and mechanisms shall be evaluated on a regular basis. If necessary, the Commission may make recommendations, whereas Member States shall present action plans on how to remedy the relevant deficiencies as identified by eu-LISA and the Commission respectively. The evaluation report by the Commission will be transmitted to several EU-institutions, including the European Parliament, the European Data Protection Supervisor as well as the FRA.

Even though reporting systems are incomparable to full judicial review, the positive effects of international review procedures are generally acknowledged.[113] Ultimately, this also applies to Art 37 of the proposal. Even though the problem of insufficient quality standards of different types of data might as such not be 'justiciable' in the traditional meaning of the term, Art 37 at least provides for the maintenance of a certain minimum level regarding such standards. Regulation 2019/817 has not changed the terminology used in the 2018 proposal (neither the terminology used in Art 13 paras 3 and 4, nor the terminology used in Art 18 para 3 and 37). On the contrary, it stresses (again) the importance of establishing the technical instruments to guarantee the quality of data gathered and entered into the different systems by EU Member States.

(2) The Right to Data Protection

[110] FRA, Interoperability and Fundamental Rights Implications, *supra* n. 12, at 13 15.

[111] Cf. M. Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Bloomsbury, Oxford Portland 2017) at 27.

[112] WP29, Opinion on Commission proposals, *supra* n. 14, at 7.

[113] Cf. W. Kälin, *Examination of State Reports*, in: H. Keller/G. Ulfstein (eds.), UN Human Rights Treaty Bodies (Cambridge University Press, Cambridge 2012) 16 72, at 17.

 DOI: 10.17103/sybil.23.4

The right to data protection can be found *inter alia* in Art 8 ECHR as a right inherent to the right to private life.[114] The right to data protection as enshrined in Art 8 FRC (as well Art 16 TFEU) is separated from the right to private life, which can be found in Art 7. The clear and distinct separation of these rights in the FRC did not change their original interrelatedness. Nowadays, however, it is understood that the right to data protection exists irrespective of any privacy concerns. Moreover, the protection of data is conceived as a mandatory prerequisite for the enjoyment of other fundamental rights, especially the right to non-discrimination. As many other fundamental rights, the right to data protection is not absolute. The FRC stresses that "[A]ny limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others." The permissibility of limiting fundamental rights for the purpose of preventing terrorist attacks or other serious crimes has been affirmed by the ECJ in *Kadi* and *Al Barakaat*[115] when the Court emphasized in both cases that the fight against terrorism constitutes a legitimate "general interest" within the meaning of Art 52 para 1 FRC. More specifically, the ECJ confirmed that the processing of data may be an adequate tool in order to maintain or re-establish public security[116]. The ECHR, on the other hand, does not contain a specific limitation clause. Permissible limitations of human rights have to be found at each individual right.[117]

The right to data protection is also enshrined in an abundance of secondary legislative acts, including the General Data Protection Regulation (GDPR)[118], the Police Directive[119] as well as Regulation 2018/1725[120]. It is the objective of the GDPR to "lay down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[121] However, the scope of the Regulation is limited. It does not apply, *inter alia*, to the processing of data "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of

---

[114] Cf. *Leander v. Sweden*, ECHR (1987), Application No. 9248/81, para 48; *M.M. v. The United Kingdom*, ECHR (2013), Application No. 24029/07. For more details, see W. Schabas, *The European Convention on Human Rights: A Commentary* (Oxford University Press, Oxford 2017) at 382 – 383.

[115] Judgement of 3 Sepetember 2008, *Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council of the European Union*, C-402/05 P and C-415/05 P, EU:C:2008:461, para 363.

[116] Judgement of 8 April 2014, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána and Kärntner Landesregierung*, C-293/12 and C-594/12, EU:C:2014:238, para 43.

[117] X. Groussot/G.T. Petursson, *The EU Charter of Fundamental Rights Five Years on: The Emergence of a New Constitutional Framework?*, in: S. d Vries/U. Bernitz/S. Weatherhill, The EU Charter of Fundamental Rights as Binding Instrument (Bloomsbury, Oxford – Portland 2015) 135 – 154, at 139.

[118] GDPR, *supra* n. 98.

[119] Directive (EU) 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 (Police Directive), OJ 2016 L 119/89.

[120] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, 2018 L 295/39.

[121] GDPR, *supra* n. 98, Art 1 para 1.

 DOI: 10.17103/sybil.23.4

criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security." With regard to these criminal matters, the Police Directive applies. In addition, Regulation 2018/1725 governs the processing of data undertaken by the European Union and its bodies respectively. This "triad" of relevant secondary acts poses another challenge for the analysis of the Commission's proposal. In its opinion of 2018, the FRA primarily criticized the proposal for two reasons. On the one hand, several provisions might be incompatible with the principle of "purpose limitation" and therefore rise strong fundamental rights concerns. On the other hand, various provisions might infringe upon the principle of so-called "data minimization".

(a) *The Principle of Purpose Limitation*

The principle of purpose limitation ranks among the most cardinal principles in European data protection law.[122] It is reflected *inter alia* in Art 8 para 2 FRC, according to which "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." Moreover, Art 5 para 1 lit b GDPR stresses that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (...)."[123]

At the outset it should be borne in mind that establishing interoperability between the different EU information systems clearly blurs the line between migration policy, border control, law enforcement and criminal investigations. Art 20 of the Commission's proposal foresees that police authorities – in case this is provided by national law – are allowed to query the CIR for the sole purpose of identifying a person (as long as the identity check takes place for the purpose of contributing to preventing and combating irregular migration and to contribute to a high level of security).[124] As already mentioned, the CIR contains different types of data, including fingerprints. At the same time, Art 20 states that Member States have to define *themselves* as to what parameters and under which circumstances Member States authorities may query the CIR within the greater framework of contributing to an increased level of security and of preventing and/or combating irregular migration.[125] The FRA argued that leaving at the discretion of the Member States to decide when the CIR can be queried is incompatible with recent jurisprudence provided by the ECJ.[126]

In *Digital Rights Ireland*, the ECJ clarified that legislative acts have to be formulated clearly, that is to say, with a sufficient level of determinacy, in case the relevant rule in question interferes (or has the potential of interfering) with fundamental rights.[127] According to the Court, "[T]he need for such

[122] Cf. Council of Europe and FRA, Handbook on European Data Protection Law, 2018 edition, at 122.

[123] For more details see Art 29 Data Protection Working Party, 00569/13/EN WP 203.

[124] Cf. Art 2 para 1 lit b and c Proposal.

[125] Cf. EDPS; Opinion 4/2018, *supra* n. 13, nn. 37 and 40.

[126] FRA, Interoperability and Fundamental Rights Implications, *supra* n. 12, at 26.

[127] *Digital Rights Ireland*, *supra* n. 115, para 46. See also Judgement of 21 December 2016, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, C-203/15 and C-698/15, EU:C:2016:970, para 122; Judgement of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14, EU:C:2015:650, para 78; Opinion 1/15 of the Court of 26 July 2017, EU:C:2017:592, para 38; Judgement of 13 September

 DOI: 10.17103/sybil.23.4

safeguards is all the greater where (...) personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data."[128] Since the Commission's proposal merely states that it is upon the Member States to establish specific rules according to which the CIR may be queried for the purpose of identifying a person, the FRA concluded that Art 20 is incompatible with the principle of purpose limitation. By the same token the EDPS stressed that the identification of a person as such "is not an end in and of itself but needs to serve a specific objective; for instance to check whether the person is wanted by the police or has the right to stay in the EU".[129] The EDPS criticized that Art 20 of the proposal is formulated too broadly as it merely refers to Art 2 para 1 lit b and c of the Commission's proposal according to which identity checks by national authorities are lawful for the purpose of preventing and combating irregular migration and contributing to a high level of security. According to the EDPS, the terms referred to in Art 2 para 1 lit b and c are too broad and require further clarification. The EDPS therefore recommended defining more clearly the terms "combating irregular migration" and "contributing to a high level of security" in the Commission's proposal.[130] Likewise, WP29 emphasized that Art 20 of the Commission's proposal allowing legislators to grant access rights for the purpose of general identity checks is highly doubtful. Precise conditions need to be established foreseeing in detail under which circumstances and according to what parameters the CIR may be queried.[131] Furthermore, the EDPS also criticized that in its original version the Commission's proposal generally allows to access the CIR in order to identify a third country national for the purpose of maintaining a high level of security. This terminology erroneously suggests the conclusion that generally third-country nationals pose a threat to security. In order to avoid this falsification, the EDPS suggested to reformulate the proposal in that such identity checks vis-à-vis third-country nationals shall only be allowed "where access for the same purposes to similar national databases exist and under equivalent conditions."[132]

It is particularly worthy of note that the Commission's original proposal foresaw identity checks based on biometric data. The EDPS emphasized that taking biometric data systematically would stigmatize third-country nationals as being a general risk to public security. He therefore suggested reformulating the Commission's proposal by stressing that biometric data shall only be used as a last resort and identity checks based on Art 20 shall only be allowed in the presence of the person concerned and only in case the person concerned is *inter alia* unable to cooperate or is not in the possession of documents proving their identity.[133] Regulation 2019/817 has been formulated differently as it now establishes concrete criteria according to which the CIR may be queried by Member States. More precisely, Art 20 states that national police forces are only allowed to access the CIR in case "a police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity."

2018 (referral to Grand Chamber on 4 February 2019), Case of Big Brother Watch and Others v. The United Kingdom, ECtHR Application Nos. 58170/13, 62322/14 and 24960/15, paras 224 – 228.

[128] *Digital Rights Ireland*, *supra* n. 115, para 46.

[129] EDPS, Opinion 4/2018, *supra* n. 13, at 13.

[130] *Ibid.*

[131] WP29, Opinion on Commission proposals, *supra* n. 14, at 21.

[132] EDPS, Opinion 4/2018, *supra* n. 13, at 14.

[133] *Ibid.* At 16 – 18.

 DOI: 10.17103/sybil.23.4

Another aspect which has been criticized by the EDPS was that according to Art 17 and 18 of the Commission's proposal, the CIR would include *inter alia* data stored in the ECRIS-TCN (conviction information on third-country nationals and stateless persons). This is particularly problematic as the CIR has been established for the purpose of facilitating the correct identification of a person as well as for the detection of multiple identities.[134] This raises the question of whether using data stored in the ECRIS-TCN for these two purposes meets the criteria of necessity and proportionality.[135] According to Art 24 para 1 Regulation 2019/816, "[T]he data entered into the central system shall only be processed for the purpose of the identification of the Member States holding the criminal records information on third-country nationals." The terminology used in the Commission's proposal establishing an interoperable IT framework goes far beyond the terminology used in Regulation 2019/816 by allowing to query the ECRIS-TCN to "detect multiple identities and to facilitate identity checks" in general. This clearly contradicts the principle of purpose limitation.[136] Regulation 2019/817 now foresees that "[A] common identity repository (CIR), creating an individual file for each person that is registered in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN containing the data referred to in Article 18, is established for the purpose of facilitating and assisting in the correct identification of persons registered in the EES, VIS, ETIAS, Eurodac and ECRIS-TCN in accordance with Article 20, of supporting the functioning of the MID in accordance with Article 21 and of facilitating and streamlining access by designated authorities and Europol to the EES, VIS, ETIAS and Eurodac, where necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences in accordance with Article 22."

(b) *The Principle of Data Minimisation*

The FRA also criticized the Commission's proposal for infringing of the principle of data minimisation, which is mentioned *inter alia* in Art 5 para 1 lit c of the GDPR.[137] Personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[138] Regulation 2018/1725, which applies to the processing of personal data by the Union institutions, bodies, offices and agencies, uses the same terminology. It is worthy of note that prior to the entry into force of the GDPR[139], the notion of "data minimisation" has not been used as a distinct term in any legislative act adopted by the

[134] Proposal Art 17 para 1.

[135] EDPS, Opinion 4/2018, *supra* n. 13, at 49 – 51.

[136] *Ibid.* At 49 – 53.

[137] See the latest judgment rendered by the ECJ, Judgement of 16 January 2019, *Deutsche Post AG v. Hauptzollamt Köln*, C-496/17, EU:C:2019:26, para 18. The ECHR has explicitly referred to the principle of data minimisation as enshrined in the GDPR as well. See *Barbulescu v. Romania*, ECHR (2017), Application No. 61496/08, para 51.

[138] Cf. N.N. Gomes de Andrade/S. Montelone, *Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications*, in: S. Guthwirth/R. Leenes/P. de Hert/Y. Poullet (eds.), European Data Protection: Coming of Age (Springer, Dordrecht 2013) at 131.

[139] Art 99 para 2 GDPR, *supra* n. 98. Regulation 2018/1725 entered into force the 20st day after its publication in the OJ, which was 21 November 2018. See Art 101 para 1 Regulation 2018/1725.

EU. The Data Protection Directive[140], which was replaced by the GDPR, used a very similar terminology but did not mention the term "data minimisation" explicitly. Everything changed with the entry into force of both the GDPR and Regulation 2018/1725, which both use the notion of "data minimisation" as a distinct term.

It should also be emphasised that the content and meaning of the principle of data minimisation changed with the entry into force of the GDPR and Regulation 2018/1725. While the previous Data Protection Directive stated that the processing of data shall be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"[141], the GDPR only allows for the processing of personal data if such processing is necessary in relation to the relevant purpose to be achieved.[142] The terminology used in the Police Directive is different. According to Art 4 para 1 lit c the processing of personal data needs to be "adequate, relevant and not excessive in relation to the purposes for which they are processed." It should be noted that all three legislative acts, the GDPR, the Police Directive and Regulation 2018/1725 apply to Regulation 2019/817. This leads to the fact that different concepts of data minimisation will apply, either the concept enshrined in both the GDPR and Regulation 2018/1725 (the concept of "necessity") or the concept enshrined in the Police Directive, clearly referring to proportionality considerations. It remains to be seen how the ECJ will react to the different wording when it comes to data protection.[143]

In substantial terms, the FRA but also WP29 criticized the processing of specific types of biometric data in the BMS. For example, the BMS stores biometric templates obtained from the SIS in the area of law enforcement,[144] which includes DNA.[145] Generally, biometric data denote "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[146] The WP29 stressed that biometric templates also constitute sensitive data despite the fact that they contain only a limited amount of personal information. Since the biometric templates stored in the BMS will be used as "universal identifiers" the WP29 suggested to treat those biometric templates just like biometric data themselves.[147] The same approach has been taken by the FRA,

[140] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 2005 L 281, no longer in force: 24/05/2018.

[141] *Ibid.* Art 6 para 1 lit c.

[142] Cf. P. Voigt/A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide (Springer, Cham 2017)* at 90.

[143] See also Art 5 lit c Convention 108.

[144] The proposal refers to the current SIS proposal. See Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, COM/2016/0883 final - 2016/0409 (COD).

[145] *Ibid.* Art 20 para 3 lit w and x.

[146] Art 4 para 14 GDPR, *supra* n. 98.

[147] WP29, Opinion on Commission proposals, *supra* n. 14, at 8.

 DOI: 10.17103/sybil.23.4

for example. It should be noted that, in principle, the GDPR does not allow for the processing of biometric data unless "the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject." That means, the processing of biometric data is subject to strict conditions. As already indicated, the main purpose of the BMS is to "facilitate the identification of an individual who is registered in several databases, by using a single technological component to match that individual's biometric data across different systems, instead of several components". Processing biometric data for the sole purpose of identifying a person may well be of "substantial public interest" within the meaning of Art 9 para 2 lit g GDPR. However, account shall be taken of the fact that some types of biometric data, such as DNA and palmprints, are only stored in the SIS. Hence, it would be technically impossible to undertake a "cross-system comparison" with regard to DNA and palmprints. In light of the wording of Art 5 para 1 lit c GDPR, the processing of such data therefore inevitably appears to be unnecessary in relation to the relevant purpose for which they are processed. Given the fact that data obtained from the SIS cannot be used for cross-checks, the criterion of necessity cannot be fulfilled. It is also worthy of note here that Regulation 2019/817 expressly states that the BMS will not process data obtained from the SIS as this would clearly constitute a violation of the principle of data minimisation.[148]

Finally, it also should be pointed out that the processing of certain types of biometric data is subject to particularly strict criteria. This holds especially true for DNA. Art 22 para 1 lit b of the Commission's latest proposal of a Regulation on the Establishment, Operation and Use of the Schengen Information System (SIS) in the Field of Police Cooperation and Judicial Cooperation in Criminal Matters stresses clearly that DNA "may only be added to alerts provided for in Article 32(2)(a) and (c) and only where photographs, facial images or dactylographic data suitable for identification are not available." Therefore, among several types of biometric data, DNA ranks among the most sensitive data which can be used for the purpose of identifying a person. This aspect has been stressed by Art 29 Data Protection Working Party in its Opinion of 2018.[149] Moreover, both the ECtHR and the ECJ have already highlighted the strict criteria which apply to the processing of biometric data in general. In *S. and Marper v. The United Kingdom*[150] the ECtHR indicated that biometric data need to be treated with increased sensitivity, especially when it comes to people who have been convicted of a criminal offence. Likewise, in *M.K. v. France*[151], the ECtHR called the preventive storing and retention of fingerprints "tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant". In *Schwarz v. Bochum*, which dealt with the storing of biometric data in relation to the issuing of passports, the ECJ indicated that especially strict criteria apply to the storing of biometric data in centralised storage

[148] See also the comments made by the EDPS, Opinion 4/2018, *supra* n. 13, at 79.

[149] WP29, Opinion on Commission proposals, *supra* n. 14, at 5 – 6.

[150] *S. and Marper v. The United Kingdom*, ECHR (2008), Applications Nos. 30562/04 and 30566/04, paras 66 – 125. Cf. F. Boehm, *Information Society*, *supra* n. 28, at 267 – 268.

[151] *MK v. France*, ECHR (2013) Application No. 19522/09, para 40.

 DOI: 10.17103/sybil.23.4

systems.[152] Overall, it can be stated that the processing of certain types of biometric data, such as DNA, is subject to strict conditions, whereas distinctly looser conditions are applied to other, less sensitive types of biometric data. This aspect will play a pivotal role in interpreting Regulation 2019/817 and the principle of data minimisation.

(D) CONCLUSION

Regulation 2019/817 and its drafting process reflect several challenges the EU and its Member States have been confronted with over the past few years. Given the increased number of migrants and refugees trying to enter the EU, specific measures were necessary in order to guarantee interoperability between the different EU information systems. As emphasized by the FRA, specific groups of people are more likely to be affected by the aforementioned measures than others. There is an increased probability that, *inter alia*, children, the disabled and people seeking international protection will be controlled at border crossings. By emphasizing explicitly that, particular attention has to be paid to such vulnerable groups and their fundamental rights and by – at least implicitly – calling upon Member States to take specific action in this respect, Regulation 2019/817 establishes an appropriately high standard of fundamental rights protection.

It should be noted that the interplay between Member States and their national authorities with EU-institutions including centralised IT systems is becoming increasingly complex. The establishment of a centralised and fully interoperable IT system at the Union level has created a dual compound of data entered into national databases, which are later transferred to a centralised EU system. Regulating such complex aspects, which almost inevitably bear the risk of infringing upon the right to data protection, requires EU legislation to lay down precise criteria governing the relevant measures in question. In its recent jurisprudence on data protection the ECJ has established such criteria. In future, the findings of the Court will play an ever important role when it comes to the interpretation and application of Regulation 2019/817. Furthermore, Member States are increasingly inclined to broaden the types of personal data that can be used for the purpose of identifying a person, especially when it comes to third-country nationals, as the recent developments with regard to the SIS clearly illustrate. The use of biometric data has always constituted a delicate matter in legal terms. The increased interest in using DNA thus has caused great concern of the FRA, the EDPS as well as WP29. At least when it comes to the sole purpose of identification, the use of DNA would not be in line with the principle of data minimization. Hence, DNA usage may only be contemplated if dactyloscopic data are unavailable and DNA is the only option to identify individuals who need to be placed under protection, such as children.

In addition to these material considerations, Regulation 2019/817 and its drafting process also illustrate clearly the significant influence the FRA, the EDPS and WP29 were/are able to exert when it comes to the awareness for and protection of fundamental rights. Evidently, the criticism expressed by the agency was taken seriously and major amendments were made prior to the final adoption of Regulation 2019/817.

[152] Judgement of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, EU:C:2013:670, paras 59 – 63.

 DOI: 10.17103/sybil.23.4

Apparently, the FRA, the EDPS as well as the WP29 were able to find a balance between rising interest for security, the increased transparentizing of individuals and fundamental rights. As a result, the relevant EU legal framework, especially the GDPR, can be understood as a normative firewall against excessive transparency and the evergrowing thirst of European institutions and domestic authorities for the collection and processing of personal data.

 DOI: 10.17103/sybil.23.4