Human Rights Law Review, 2021, 21, 433–457
doi: 10.1093/hrlr/ngaa057
Advance Access Publication Date: 8 February 2021
Article

OXFORD

Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU

Cristina Blasi Casagran*

ABSTRACT

On 11 June 2019, two Interoperability European Union (EU) Regulations entered into force. With it, six existing EU databases created for security and border management purposes merged into one single, overarching EU information system operating with the purpose of changing the way front-line officers worked in various tasks. The main objective of these Regulations was to prevent and combat illegal immigration and to improve security within the Area of Freedom, Security and Justice of the Union. This article studies the challenges that have emerged from making EU databases and information systems 'interoperable' as well as the potential negative consequences that the Regulations may have for fundamental rights as enshrined in the EU Charter of Fundamental Rights. In particular, it examines whether the interoperability between EU information systems could violate the rights related to data protection, rights of the child, prohibition of discrimination as well as principles of necessity and proportionality.

KEYWORDS: interoperability, EU information systems, fundamental rights, data protection, migration, security

1. INTRODUCTION

M.A. is a thirteen-year-old Syrian boy who has managed to get to the Greek border looking for safety and a better life. His parents could not travel with him, so he is an unaccompanied minor arriving in the European Union (EU). At the border, Greek authorities check his passport, collect his fingerprints and introduce his personal details into their system. At the click of a button, they are able to check whether he has applied for asylum before; whether he has any previous criminal records; whether police are actively searching for him and even how many times he has entered the EU before (with visa and without). Although he has no criminal records and is not sought by police, a search 'hit' in one of the connected databases alerts the border guard that he has been

* Assistant Professor, Serra Húnter, Autonomous University of Barcelona, Spain.

denied asylum in the EU. Thus, his fate is sealed—he faces the choice of a forcible return to Turkey or a precarious life in limbo living as an irregular migrant in Greece.

Situations like these are now possible in the EU as the Interoperability Regulations ((EU) 2019/817 and (EU) 2019/818) entered into force in the EU in 2019.[1] These two Regulations (hereinafter, the Regulations or the Interoperability Regulations) establish a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum migration, borders and visa. Since the idea of these Interoperability Regulations was first introduced by the European Commission in a Communication in 2016,[2] they have raised many fundamental rights concerns, as they seek to centralise data from six existing and forthcoming EU information systems for security, border and migration management. The main objective is to prevent and combat illegal immigration and to improve security within the Area of Freedom, Security and Justice (AFSJ) of the Union. Therefore, it is not surprising that the Regulations include legal bases from both the chapter of 'border control, asylum and asylum policy'[3] and also the 'police cooperation policy'.[4] By combining these two types of legal bases, the EU can treat the objective of border management and the objective of police cooperation as one single general purpose. Yet, by interconnecting six databases under one single purpose, these Regulations may be infringing the right to data protection and other fundamental rights.

This article clarifies the scope and linkage between six existing EU information systems and the new interoperability components. It argues that there are two sides of the coin to be considered: on the one hand, it will enhance the cooperation and efficiency between migration agencies, police forces and judicial bodies. On the other hand, without the right safeguards in place, it could become a dangerous tool against fundamental rights, as centralising databases could increase the risk of abusing the system for purposes beyond the original intent.

2. SCOPE OF THE SIX EXISTING EU INFORMATION SYSTEMS

The Interoperability Regulations provide a mandate to interconnect the following EU information systems: (a) the Entry/Exit System (EES), (b) the Visa Information System (VIS), (c) the European Travel Information and Authorisation System (ETIAS), (d) Eurodac, (e) the Schengen Information System (SIS) and (f) the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN). These six systems all have key similarities in common; namely, that they primarily—but not

1 Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between the 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 [2019] OJ L 135/27; Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between the 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 [2019] OJ L 135/85.

2 Communication from the Commission to the European Parliament and the Council. 'Stronger and Smarter Information Systems for Borders and Security', 6 April 2016, COM(2016) 205 final.

3 Articles 77–80 TFEU.

4 Articles 87–89 TFEU.

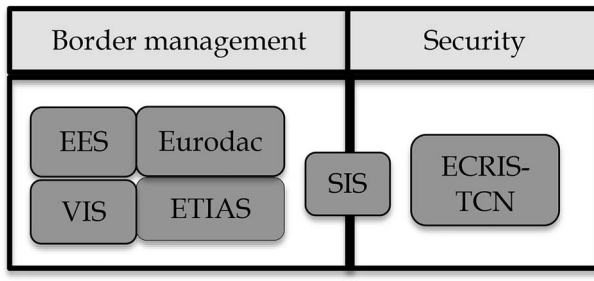

Figure 1. Main purposes of the six interoperable information systems.

exclusively—relate to third-country nationals and that they collect similar types of biographic and biometric data. As established in Figure 1, some of them were created for border management purposes, whereas others were originally built for security purposes.

Regarding VIS, it was created in 2004 with the purpose to strengthen the immigration policy of the EU through a common data identification system in all Member States for short-term visas to stay for up to 90 days. The specific objectives of VIS were basically (a) facilitating the visa application procedure, (b) preventing the so-called 'visa shopping', (c) promoting the fight against fraud, (d) promoting external border controls between Member States, (e) assisting in the identification of persons with access denied in the territory of the Member States, (f) facilitating the application of the Dublin II Regulation and (g) contributing to the prevention of threats to the internal security of some of the Member States. The 2008 Council Decision[5] extended this scope by expanding data access to further relevant national and EU bodies.[6] Since May 2018, there is a new proposal for a regulation, which extents this scope to include the databases of long-stay visas and residence permits, decreases the age for the inclusion of biometrics in the system from 14 to 6 years old and includes a facial image and two fingerprints of the holder.[7]

As a way to complement the VIS, the EES was adopted in 2017.[8] It collects data from non-EU nationals and traces their entry and exit records with the purpose of facilitating border crossing of *bona fide* travellers, identifying visa over-stayers and also permitting law enforcement authorities access to travel history records. The VIS does not automatically calculate the duration of time a short-stay visa-holder remains

5 Council Decision 2008/633/JHA of 23 June 2008 on access to consult the VIS by the designated authorities of the Member States and by Europol, with purposes of prevention, detection and investigation of terrorism and other crimes serious crimes [2008] OJ L 218/129.

6 Blasi Casagran, *Global Data Protection in the Field of Law Enforcement: An EU Perspective* (2016) at 130–131.

7 Proposal for a Regulation of the European Parliament and of The Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, 16 May 2018, COM(2018) 302 final.

8 Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an 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 [2017] OJ L 327/20.

in the Schengen area, so this task is purely conducted by checking the entry and exit stamp(s) placed in the passport of the traveller. Thus, the EES will replace this mechanism of manual stamping of passports that is used today at the border controls and instead a record of all cross-border movements of third-country nationals will be created via the collection of alphanumeric and biometric data. The time, date and location of an individual's border crossings will be registered in a centralised database.

Another new database for border management is the ETIAS. This is a very new system, as it was adopted in 2018,[9] and it is still being implemented by the Member States. Once it becomes operational, it will collect information on all travellers who are entering visa-free to Europe (estimated as 39 million every year)[10] with the purpose to control and prevent irregular migration prior to travel to the Schengen area. ETIAS aims to contribute to a more efficient management of the EU's external borders, improving internal security and facilitating a better management of irregular migration.

Within the field of asylum, Eurodac was born as a result of the agreement signed in 2003 amongst the EU Member States, through which asylum applications should be processed in the country where the applicants first declare their intention to seek asylum.[11] Eurodac stores fingerprints of asylum seekers (known as 'Category 1'), individuals connected with irregular border-crossings ('Category 2') and third-country nationals or stateless persons found to be irregularly staying in a Member State ('Category 3'). In 2016, a proposal, which is still under negotiation, established that the personal data of such individuals would be retained for 5 years, the age limit for data collection in all three categories would be lowered from 14 to 6 years old and that the system would include facial recognition software.[12]

As regards the SIS, this database has hybrid purposes within the scope of border management and security. SIS origin is situated in 1985 with the adoption of the Schengen Agreement. This agreement was a milestone for the European policy against terrorism, as its main goal was to control the external borders of the Member States and, specifically, the third-state nationals entering European territory. SIS allows Member States to transfer quickly and effectively all information on border controls and displacement of people. Through the SIS—operational since 1995—Member States can send and receive alerts about people who have an arrest warrant, are linked to

9 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 ETIAS [2019] OJ L 236/72.

10 European Commission, Technical Study on Smart Borders [2014] DG HOME, available at: www.ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf [last accessed 29 October 2020].

11 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.

12 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.

police investigations or criminal proceedings or are denied access to the Schengen area. It also reports on vehicles, weapons of fire, identity documents and bank checks classed as missing or stolen. Searches via SIS can issue a positive response or 'hit', which specifies the action to be taken against people identified as being banned from entering the Schengen area. Due to the technological progress, SIS has evolved to the second-generation SIS (SIS II),[13] which introduces the possibility of collecting biometric data, such as fingerprints or photographs of individuals. SIS II is the EU's largest database and information system for law enforcement and migration purposes, which now includes all return decisions issued by national authorities, any checks carried out by the officials and offender DNA profiles.

Finally, the ECRIS is a decentralised electronic system with the purpose of exchanging criminal record information between national authorities of the EU Member States. It grants access to judges, prosecutors and other relevant authorities to vast amounts of information on a subject's criminal history regardless of the country where that individual was previously convicted. It has now been expanded to include a centralised database called ECRIS-TCN, which processes information on previous convictions of third-country nationals and stateless persons.[14]

Each of these EU information systems has their own specific purpose related to border management or security, but they all have the identification of 'illegally staying third-country nationals' as the common ancillary purpose. Also, it is relevant to mention that some of these EU information systems are newer than others: EES, ETIAS and ECRIS-TCN are still in the phase of being implemented, whereas SIS, VIS and Eurodac are well-established tools for many years now, but they have expanded their scope and purposes over the years.

3. NEW SCOPE AND PURPOSES OF THE INTEROPERABILITY SYSTEM

For border and law enforcement authorities, one of the problems of having numerous information systems is that end-users have to visit so many databases from which they will receive overlapping and delayed information.[15] Yet the idea of creating one single,

13 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the 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 [2018] OJ L 312/56; Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the SIS for the return of illegally staying third-country nationals; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the SIS in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 [2018] OJ L 312/1.

14 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 ECRIS and amending Regulation (EU) 2018/1726 [2019] OJ L 135.

15 Gutheil, 'Interoperability of Justice and Home Affairs Information Systems' (2018) *Civil Liberties, Justice and Home Affairs* PE 604.947 at 40.

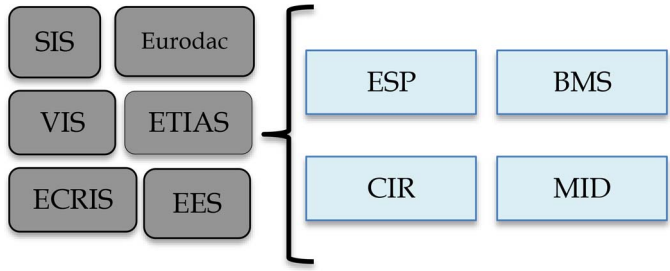

Figure 2. Information processed by the interoperability components.

overarching EU system that merges data from the six existing databases goes beyond the need to solve these (minor) procedural controversies, and it has been perceived as controversial from a fundamental rights' perspective.

The ambitious goal of the Interoperability Regulations covers six specific but challenging purposes: (a) increasing the effectiveness of border checks, (b) helping to prevent and combat irregular migration, (c) reinforcing the level of security within the EU, (d) promoting the implementation of the common visa policy, (e) detecting, preventing and investigating terrorist and other serious crimes and (f) helping identify unknown and undocumented persons.[16]

To achieve these objectives, the six above-mentioned large-scale databases are merged and crosschecked through four new components: The European search portal (ESP), the shared biometric matching service (BMS), the common identity repository (CIR) and the multiple-identity detector (MID).

Each of these four interoperability components has been created for a specific purpose:[17] the ESP will enable the searching of alphanumeric or biometric data through the six databases, plus Interpol and Europol data; the shared BMS will extract biometric 'templates'[18] from each of the six EU databases with the purpose of facilitating the searching and cross-matching of the biometric data; the CIR will store the biometric and biographic data of non-EU nationals, collected via Eurodac, the VIS, EES, ETIAS and ECRIS-TCN;[19] and the MID will make 'identity confirmation files' whenever a new file is created or updated in the EES, VIS or ETIAS, and an alert on a person is

16 Interoperability Regulations 817 and 818, supra n 1 at Article 2(1).

17 See Blasi Casagran, supra n 6 at 23–26; Blasi Casagran, 'Límites del derecho europeo de protección de datos en el control de fronteras de la UE' (2015) *Revista CIDOB d'Afers Internacionals* 111 at 129–130; Tomaszycki, 'The Interoperability of European Information Systems for Border and Migration Management and for Ensuring Security' (2018) 12 *Law and Politics* 3.

18 For further information about the definition of 'biometric templates', see Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and 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 and Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), 12 December 2017, SWD/2017/0473 final.

19 In the cases of the SIS, Interpol and Europol data, the identity data will not be stored in the CIR but in the information systems themselves.

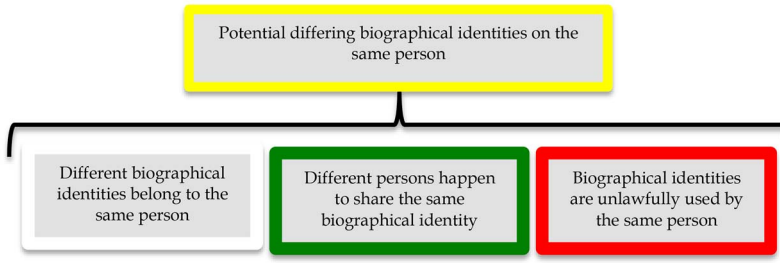

Figure 3. Four possibilities of links that need to be verified through MID.

created or updated in the SIS, or a new record is created or modified in the ECRIS-TCN. The MID will store links between the individuals present in more than one of these systems, and these links will be labelled in four categories: white, yellow, green and red.[20] A yellow link will be created when a query of biometric or identity data leads to one or several hits where the identity data of the linked files cannot be considered as similar.

When using MID, police officers will need to manually verify a yellow link that flags when, for instance, a name and surname is introduced to SIS and the same name has also been found in EES, ETIAS or VIS. As shown in Figure 3, the police officer then checks through the MID to find whether (a) the linked data refer to legally distinct persons who have a very similar name (shown in green), (b) the linked identities refer to the same person legally (shown in white) or (c) the identity data refer unlawfully to the same person (shown in red).[21] Regarding the latter, the main goal of the MID is to provide a response to the problem of identity fraud committed by some non-EU nationals.[22]

As far as fundamental rights are concerned, one issue to be raised on these new four components is that their existence exceeds the concept of 'interoperability' as such.[23] Although the concept 'interoperability' is not explicitly defined in any of the official EU documents and can have several dimensions,[24] it should be technically understood as 'the ability of different information systems to communicate, exchange data and use the information that has been exchanged'.[25] The Regulations refer to them as 'components'

20 Interoperability Regulations 817 and 818, supra n 1 at Articles 30–33.

21 SIS Regulation, supra n 8 Articles 30–33; Gutheil, supra n 15 at 65.

22 Impact assessment, supra n 18 at Section 6.1.8.4.

23 Gutheil, supra n 15 at 13; Bunyan 'Analysis: The "Point of no return" Interoperability morphs into the creation of a Big Brother centralised EU state database including all existing and future Justice and Home Affairs databases' (2018) *Statewatch* at 14; Council of the European Union, Opinion on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 10484/18, 27 June 2018.

24 Goddard, 'Understanding the Challenge of Legal Interoperability in Coalition Operations' (2017) 9 *Journal of National Security Law & Policy* 211; In this sense, Gutheil, supra n 15 at 44 refers to four layers of interoperability: legal, organisational, semantic and technical.

25 Definition from European Court of Auditors, 'EU information systems supporting border control—a strong tool, but more focus needed on timely and complete data' (2019) Special Report n 20 at 45. A similar definition has been previously used by the Commission in Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies

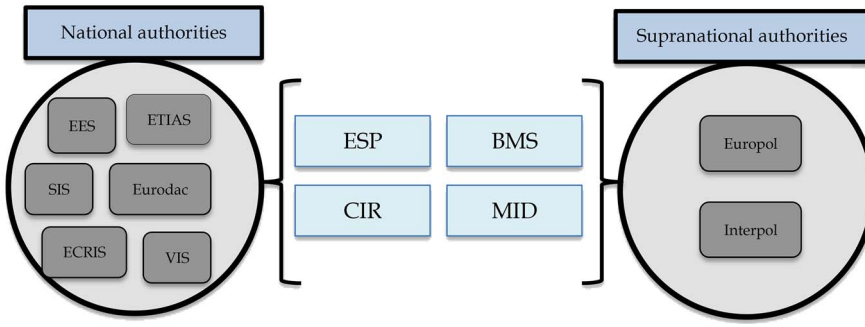

Figure 4. Authorities authorised to access the interoperability components.

or 'repositories' but they should in fact be treated as new databases. On the one hand, they will be processing and storing data in a structured manner, so this proves that they will be more than just accessories of the EU information systems. On the other hand, these four components incorporate new objectives (e.g. identification of fraud) that are not described in the existing EU information systems, so they seem to go well beyond mere interoperability components.[26]

Another issue to be highlighted is the competent authorities which will have access to these four new components. They will be accessible fundamentally to the border and law enforcement authorities from the Member States with access to at least one of the six EU information systems. Moreover, two supranational authorities, Europol and Interpol, will have access to the components.[27] Therefore, by introducing data from an individual, these authorities will be able to simultaneously visit EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, the CIR, Europol data and the Interpol databases.

In the case of national authorities, these can include, for instance, officers in charge of registering migrants carried out by front-line border checks or border officials handling visa applications. These individuals will be able to access all existing police and border management databases before accepting migrants in the EU territory,[28] or before granting a visa. The interoperability system can be also used by police authorities within a Member State if they are unable to identify a person due to a lack of a travel documentation, or where there are doubts about the data provided by that person. In such cases, police officers will be able to query the CIR in order to identify the person, capturing fingerprints using live-scan fingerprinting techniques.[29] Police officers will also be able to access information in EES, VIS, ETIAS or Eurodac in the pursuit of criminal investigations. The only access requirement is that there should be reasonable

amongst European databases in the area of Justice and Home Affairs, 24 November 2005, COM (2005) 597 final at 3.

26 Gutheil, supra n 15 at 63; Vavoula, 'The "Puzzle" of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection' (2020) *European Law Review* 3 at 370.

27 Interoperability Regulation 818, supra n 1 at Article 7(1).

28 Council of the European Union, Implementation of Interoperability-Exchange of view, 11,847/19, 25 September 2019 at 2.

29 Interoperability Regulation 818, supra n 1 at recital 28.

grounds to believe that the consulting the EU databases will contribute to the prevention, detection or investigation of terrorist offences or other serious criminal offences.[30] This could be a mere suspicion that a person registered in any of these databases is a suspect, perpetrator or victim of a terrorist offence or other serious criminal offence.

These new access conditions go beyond what border and police officers can do at the moment and could violate the access limitation principle within the right to data protection. Today (and until the new components are operational), designated Member State authorities who wish to verify the identity of a person first have to conduct a search of their national databases. Only if they meet the conditions explicitly prescribed in relation to each EU information system, can they submit a reasoned request to the verifying authority/central access point justifying the necessity of access for each individual EU system.[31] In contrast, the new interoperability components will allow competent authorities to directly send a query for identification (using biometric or biographical data of a person) without any prior justification. If there is a 'hit-flag', only then will they need to request full access to the data contained in the EU information systems.

This is only one example of many concerns raised from these Regulations. The following sections identify several other problems related to their implementation (Section 4) as well as potential violations of EU fundamental rights (Section 5).

4. IMPLEMENTATION CHALLENGES

The Interoperability Regulations are supposed to become fully operational by 2023, and therefore, its adequate implementation has been one of the key priorities for the Romania, Finland and Croatia (2019–20) presidencies of the Council.[32] During the implementation process, the Commission and the Member States are constantly monitoring the programme to ensure that the national technical, political and economic challenges are overcome. In this sense, the Commission has started to offer forums, trainings and seminars for border/security authorities and other 'Interoperability Ambassadors' in order to ensure that the implementation of the new architecture for EU information systems is achieved in time.[33] However, some Member States, EU institutions and bodies have expressed doubts that the project could be fully implemented by 2023 due to the amount of training needed and several other potential problems.[34] Firstly, as detailed in Section 2 of the present study, two of the six interconnected EU information systems are still in their development phase at the moment (ETIAS and EES),[35] two are

30 Ibid. at recital 31.

31 Gutheil, supra n 15 at 54.

32 Council of the European Union, supra n 28 at 2.

33 Council of the European Union, Implementation of Interoperability. Exchange of views, 12,429/19, 1 October 2019 at 4–5.

34 Ibid. at 1–5; EESC, Opinion of the European Economic and Social Committee on 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, 10 August 2018 at 54.

35 The ETIAS is due to come into operation in 2020 and the EES in 2021.

currently under revision (VIS[36] and Eurodac[37]) and SIS and ECRIS-TCN have been recently adopted but their implementation is still pending. Most of the laws regulating these systems include interoperability provisions,[38] but the fact that the 'foundations' of the new Regulations do not exist yet may give rise to shortcomings in building such structures further down the line.[39] In addition, the new infrastructure will require a high number of technical experts developing IT systems, who will have to work closely with the end-users (police and border officers). [40] These will need to receive specific training on how to collect and register data in a way that can be easily interpreted in all Member States. This will be a challenge not only at a linguistic level but also from a cross-sectoral point of view. For instance, the technical knowledge and practices of an officer managing borders in the South of Spain may not be the same as the knowledge and technical expertise learned by a border authority in Finland. Therefore, common terms, capacity and knowledge should be uniformly incorporated for all end-users of the new interoperability components.

Finally, the Interoperability Regulations require the need to adopt delegated acts and implementing acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) to specify several technical aspects related (e.g. issues related to user profiles and the maintenance of existing access rights). An 'Interoperability Committee' and an expert group will be created and supported by the Member States. Although the work on these implementing and delegated acts has already started,[41] it is improbable that the four interoperability components will be achieved by 2023, as by December 2020,[42] the required delegated acts and implementing acts have not yet been adopted.

5. POTENTIAL VIOLATIONS OF FUNDAMENTAL RIGHTS

The complexity of the Interoperability Regulations may have negative implications on at least four fundamental rights as enshrined in the Treaty of Lisbon, the EU Charter of Fundamental Rights and the general principles of the EU law: (a) the privacy and data protection rights, (b) the non-discrimination principle, (c) the protection of children and (d) the proportionality principle.

A. Privacy and Data Protection Implications

The right to privacy and the right to data protection are stated in Articles 7 and 8 of the EU Charter of Fundamental Rights. These rights apply to any person within the

36 Interinstitutional negotiations are still ongoing on the May 2018 proposal to strengthen and upgrade the existing VIS.

37 An agreement is still pending on the May 2016 Commission proposal to extend the scope of Eurodac by storing also fingerprints and relevant data from illegally staying third-country nationals.

38 ETIAS Regulation, supra n 15 at Articles 11, 12, 20 and 23; Proposed Eurodac Regulation, supra n 13 at recital 14; Proposed VIS Regulation, supra n 11 at Articles 1 and 22; EES Regulation, supra n 17 at Articles 8, 36, 37 and 61.

39 EESC, supra n 34 at 52.

40 Council of the European Union, supra n 28 at 2.

41 Council of the European Union, supra n 33 at 3.

42 See Interinstitutional register of delegated acts, available at: www.webgate.ec.europa.eu/regdel/#/home [last accessed 7 December 2020].

territory of the EU regardless of whether they are EU citizens or third-country nationals. However, this section gives evidence that third-country nationals may suffer infringement of privacy and data protection rights once the interoperability components starts running.

(i) Violation of data protection principles

The General Data Protection Regulations (GDPR) establishes in Article 5 that any legal instrument regulating the processing of personal data (e.g. the Interoperability Regulations) needs to comply with the seven core data protection principles: (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimisation; (d) data accuracy; (e) storage limitation; (f) data integrity and confidentiality and (g) accountability.[43] Similar principles are included in the Directive 2016/680 on the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[44] The Interoperability Regulations include several provisions regarding the protection of personal data.[45] Yet, this section questions the conformity of these Regulations and five of these seven basic data protection principles: fairness and transparency; purpose limitation; data minimisation; data accuracy and storage limitation.

For the principle of fairness and transparency, these two notions should be assessed separately. On the one hand, the principle of fairness refers to the use of personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. This principle may be jeopardised because the new interoperability system will make data from the existing data systems accessible to a wider number of authorities, other than those bodies collecting and using the data in the first place. Today, each of the six existing databases grants access to specific authorised users within the competent national authorities and under certain conditions/limitations.[46] For instance, ETIAS is accessible by border guards and air carriers; EES grants access to visa authorities, border guards and asylum authorities and ECRIS limits its access to police and judicial authorities.

Yet, with the Interoperability Regulations visa authorities, border guards, asylum authorities, police forces, customs authorities, judicial authorities, vehicle registration authorities and air carriers will have access to all six interoperable databases regardless of whether they are originally listed as competent authorities in that EU database. This is illustrated in Table 1 below.

43 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) [2016] OJ L 127/1 at Article 5.

44 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 [2016] OJ L 119/89 at Article 4.

45 Interoperability Regulation 818, supra n 1 at Article 23 (data retention), Article 37 (data quality), Article 40–41 (data controller/processor), Article 42 (data security), Article 47–48 (individual rights).

46 European Commission, EU Information Systems. Security and Borders, December 2017.

Table 1. Authorities with access to the existing EU information systems.

The fairness of the Interoperability Regulations is questionable due to the extensive number of authorities and other authorised personnel who will be able to access all sorts of personal data. Competent authorities are not listed in the Regulations and instead will be designated by the Member States according to their national procedures,[47] so Member States have some margin of interpretation to decide who will have access. In the case of police forces, the margin may be even wider as Article 4(19) of both Interoperability Regulations states that 'police authority' means the competent authority as defined in Article 3(7) of Directive (EU) 2016/680. It includes (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences.

By such broad definition, the Regulations clearly allow police authorities to access EU information systems that are not exclusively established for purposes of prevention, detection or investigation of serious crime.[48] Also, if there is a match in the CIR, such competent authorities will be able to designate further authorised end-users to access EU information systems resulting from the query.[49] The only requirement established by the Regulations is that the national procedures and laws for granting access comply with the principle of proportionality, which is questioned in Section D below. Therefore, the extensive number of authorities which will be given access to the CIR for carrying out identity checks may lead to an unfair processing of data, causing detriment to the individuals concerned.

On the other hand, linked to the fairness principle, the transparency principle means that the processing needs to be clear, open and honest about who and how data

47 Interoperability Regulation 818, supra n 1 at recital 30.
48 Ibid. at recital 25.
49 Ibid. at recital 32.

are processed. This principle is also endangered for the wide number of unidentified authorities that will have access to the system. Particularly worrying is the lack of information on the use of the multiple-identity detection tools. The MID will create links via automated processes, creating a lot of simplicity for the end-users,[50] but there is no explanation on how such automated processes will be supervised by humans. The GDPR and Regulation 2018/1725[51] establish that decisions based solely on automated processing (with no human intervention) should include suitable measures to safeguard the data subject's rights, but no specific procedures to achieve it are detailed in the Interoperability Regulations. Therefore, more transparency is needed in this regard.[52]

The purpose limitation principle, ensuring the purposes for the processing are reasonable and clearly specified, may also be breached. As explained in Section 2, each of the existing EU information systems was separately created for a specific goal. These individual purposes conform Article 5(1)(b) of the GDPR, which states that personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'. Yet, the Interoperability Regulations establish seven new objectives,[53] enclosed into the broad purpose of 'migration management and management of internal security'. Such a wide scope has negative implications for the purpose limitation principle: first of all, as mentioned above, the new system does not only seek to improve the interoperability between existing databases but it adds new purposes for using these systems,[54] like the combat of identity fraud. This purpose should be listed in the existing EU information systems that will become interoperable. Therefore, the original databases (Eurodac, SIS, VIS, EES, ETIAS and ECRIS) should be redesigned to include new secondary objectives, like the identification of third-country nationals.[55] Yet, this formal shortcoming has to be assessed with a more substantial concern: The new identification purpose is not sufficiently justified. In this sense, the European Data Protection Supervisor (EDPS) has reminded us that the identification of a person is not an end in itself but must serve a specific objective.[56] This new purpose might invite border control and law enforcement authorities to perform routine queries using all available data, without having to demonstrate the necessity to access the identity data or that the information would aid in the investigation of a specific case.

Secondly, another violation of the principle of purpose limitation may be caused by the blurry boundaries between migration management and fight against crime and terrorism. For instance, if a police officer is looking for a criminal suspect, immediate access to information gathered for non-policing purposes (e.g. processing of asylum

50 Council of the European Union, Automation of information exchange in a strategic context—Discussion paper, 11434/19, 6 September 2019 at 5.

51 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] OJ L 295/39.

52 EDPS, Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 16 April 2018 at 21; Gutheil, supra n 15 at 53.

53 Interoperability Regulation 818, supra n 1 at Article 2.

54 Gutheil, supra n 15 at 54 and 56; Vavoula, supra n 26 at 369.

55 Gutheil, supra n 15 at 62.

56 EDPS, supra n 52 at 13.

claims or border management) will be possible. This will entail a disproportionate intrusion for travellers who agreed to their data being processed to obtain a visa or other migration purposes.[57] Also, this fusion of purposes contravenes the CJEU case-law. In *Digital Rights Ireland*,[58] the Court held that Directive 2006/24 failed to

> lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences[59]

by just referring 'in a general manner to serious crime, as defined by each Member State in its national law'.[60] In this case, the court found that the purpose for the access and use of the data was not strictly limited to the aim of preventing and detecting specific serious offences or for use in pursuing criminal prosecutions. This same conclusion may apply for the Interoperability Regulations regarding the broad general purposes it serves.

Concerns are even more striking if other EU databases join the interoperability components in the future. Specifically, the Commission and the Council are studying the possibility to combine the Prüm, the Passenger Name Record (PNR) and the Advance Passenger Information queries with those made under the interoperability components.[61] This is particularly worrisome considering that the scope and purpose of these three decentralised systems differ substantially from those of the six current integrating systems. Whereas EES, ETIAS, ECRIS-TCN, VIS, SIS and Eurodac are managing data from third-country nationals entering the EU, PNR and API will process data from EU citizens travelling to another Member State. In addition, the Prüm system is a particularly sensitive database as it shares DNA, fingerprints and vehicle registration data to law enforcement authorities within the EU[62] and will also include facial recognition technology in the future.[63] Consequently, the candidate databases would bring lot more data on EU citizens into the picture[64] and would significantly extend the scope and purpose for which this interoperability system was designed, from controlling the external borders to controlling also the internal borders of the Member States.

The data minimisation principle could also be infringed due to the vast amount of data categories collected. Article 5(1)(c) of the GDPR establishes that the processing of personal data has to be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. The CIR will store 18 types of data collected from one or more of the six existing EU information systems: (a) first name(s),

57 Ibid. at 9 and 15.

58 Joined Cases C-293/12 and 594/12 *Digital Rights Ireland ltd and Seitlinger and Others* [2014] ECR I-238.

59 Ibid. at para 60.

60 Ibid.

61 Council of the European Union, supra n 50 at 5–6.

62 Blasi Casagran, supra n 6 at 17–18.

63 Council of the European Union, Next generation Prüm (Prüm.ng)—Reports from focus groups/Report on face recognition, 13356/19, 30 October 2019.

64 Jones, 'Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status' (2019) *Statewatch and Platform for International Cooperation on Undocumented Migrants* at 15.

(b) surname(s), (c) former surname(s), (d) name at birth, (e) previous names, (f) previously used names, (g) aliases and pseudonyms, (h) parents' first names, (i) date of birth, (j) place of birth, (k) nationality, (l) sex, (m) gender, (n) type/number of travel document, (o) issuing country code of travel document, (p) validity of travel document, (q) facial image and (r) fingerprints. If a police officer seeks to identify someone and introduces one of these 18 categories in the shared container (CIR) and there is a hit, onward access will be granted to the six EU information system(s) to which the additional 17 categories of data belong. It is hard to justify that 18 categories of identify information is the minimum amount of personal data police officers will need to fulfil identification purposes. For instance, one may wonder whether is necessary to collect 'sex' and 'gender' data as two different items, or how relevant it is to gather the parents' names. Moreover, the collection of biometrics seems also excessive. The only case in which it would be justified is when the identification is to be conducted with an undocumented person, who would otherwise be impossible to identify through alphanumerical (i.e. documented) data. Otherwise, facial images and fingerprints should be removed from the list. In this sense, the 'Article 29 Working Party' has also questioned the storage of biometric templates in the BMS, stating that

> the pure facilitation of searching and matching procedures cannot be sufficient to prove the strict necessity of an additional storage, especially with regard to the strengthened requirement of data minimisation provided in the GDPR.[65]

Another data protection requirement that is not adequately applied is the data accuracy principle. Certainly, the new interoperability system will enhance the awareness amongst law enforcement authorities of alleged data input errors and inaccuracies in alphanumeric data, especially through the incorporation of the Universal Message Format (UMF).[66] Also, the CIR intends to minimise potential errors associated with the identification process by registering the following information for each person: (a) identity data, (b) travel document data and (c) biometric data.[67]

However, the responsibility for underlying data quality lies with front-line officers from each Member State, and they still can make mistakes while inserting names, addresses, ages, date of birth, types of crimes committed, etc.[68] Some Member States are more rigorous than others in inserting alerts, and there are also different thresholds

65 Article 29 Data Protection Working Party 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, WP266, 11 April 2018 at 8. The Article 29 Data Protection Working Party was independent body that dealt with issues relating to the protection of privacy and personal data in the EU until 25 May 2018.

66 Interoperability Regulation 818, supra n 1 at Article 38.

67 Ibid. at recital 22.

68 Au-Yong Oliveira, 'Recent developments of interoperability in the EU Area of Freedom, Security and Justice: Regulations (EU) 2019/817 and 2019/818' (2019) 5 *UNIO—EU Law Journal* 2 at 130.

across Member States for entering data.[69] The FRA[70] and the Commission[71] have reported poor data quality in Eurodac, VIS and SIS II, but the only official governance and control at the EU level is conducted by the eu-LISA.[72] In fact, according to the eu-LISA's own automated data quality checks and reports on data quality indicators for SIS II, there are about 3 million warnings of potential data quality issues every month. However, neither eu-LISA nor the Commission have any enforcement powers to ensure that the Member States act to correct these data quality issues in a timely manner.[73]

Hence, although the Regulations will require automatic quality checks before introducing data,[74] errors can still occur if the national officers register partial-/low-quality fingerprints, or if personal data referring to the same person are stored in two or more EU information systems under different or incomplete identities. In fact, only a few of these cases of false matches would diminish the whole effectiveness of the system. Therefore, better data quality standards centralised at the EU level should be introduced in order to improve the completeness, accuracy and reliability of data within the information systems.

Finally, regarding the storage limitation principle, there are concerns as regards the CIR and the MID. As for the CIR, the Interoperability Regulations state that personal data recorded in the CIR will be kept for 'no longer than is strictly necessary for the purposes of the underlying systems' and will be automatically deleted when the data are deleted from the original system.[75] Thus, for instance, if the personal data are deleted from the SIS, they must be removed from the CIR. Yet, the Regulations do not specify the method of deletion of data after their expiration. As a result, there is a very real risk that automatic deletion is technically not enforced by the specific system.[76] Moreover, since each EU information system has its own retention periods (10 and 2 years for Eurodac, 5 years for VIS, 3 years with possibility of extension for SIS II, etc.),[77] if data from a third-country national are found in several databases, the retention will be tied to the time limit which allows the longest time of data retention.[78] This practice infringes the data retention principle as established in Article 5(1)(e) of the GDPR.

69 Vavoula, supra n 26 at 365; European Court of Auditors, supra n 25 at 31; Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Articles 24(5), 43(3) and 50(5) of Regulation (EC) No 1987/2006 and Articles 59(3) and 66(5) of Decision 2007/533/JHA, 21 December 2016, COM(2016) 880 final.

70 FRA, *Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security* (May 2017).

71 Report from the Commission, supra n. 69; Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the VIS, the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation.

72 Interoperability Regulation 818, supra n 1 at recital 48; Regulation (EU) No 2018/1726 on the European Union Agency for the Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice (eu-LISA) [2018] OJ L 295/99 at Article 12.

73 European Court of Auditors, supra n 25 at 30.

74 Interoperability Regulation 818, supra n 1 at Article 13(3) and Article 37.

75 Ibid. at Article 35.

76 EDPS, supra n 52 at 21; EESC, supra n 34 at 53.

77 See Table 1.1 of Blasi Casagran, supra n 6 at 48.

78 Meijers Committee, Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017 [2018] CM1802 at 5.

Table 2. Collection of biometrics by the EU information systems.

BMS						
Type of biometrics	SIS	VIS*	EES	ECRIS-TCN	ETIAS	Eurodac
Facial images	X		X			
Fingerprints	X	X	X**	X		X

*Although the VIS does not collect facial images at the moment, the Council has proposed an amendment for the proposed VIS Regulation suggesting that the visa procedure and the VIS should benefit from the technology developments related to facial image recognition and taking live facial images as part of the short stay visa procedure. See Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA—Presidency compromise proposals regarding the recitals, 13799/18, 5 November 2018.

**Only for those individuals who have been refused entry regardless of whether they are visa-obliged or visa-exempt subjects.

(ii) Risks linked to the processing of biometric data

Biometrics, unlike other types of data, are inherent' to the body itself and refer uniquely and permanently to a person. They have proven to be an effective method of authenticating an individual's identity, as their uniqueness enormously reduces the risk of errors associated with more than one person with the same or similar alphanumerical personal data. Their processing shall be in principle prohibited unless one of the exceptions of Article 9 GDPR applies, as it poses unique threats in terms of privacy and data protection for their very sensitive nature. One of the exceptions is that 'the processing is necessary for reasons of substantial public interest'.[79] However, for these situations, the CJEU and the ECtHR have repeatedly warned that the storage of biometrics needs to comply with more stringent requirements and additional specific guarantees (e.g. effective right of deletion) than that of alphanumerical personal data.[80]

Biometrics will be processed by three of the four new interoperability components: the BMS, the MID and the CIR. Whereas the BMS will process biometric data to detect multiple identities from all existing and new systems (except for ETIAS);[81] the MID will search across the biometric and biographic data from all existing systems simultaneously; and the CIR will facilitate and assist in the correct identification of persons, using such biometric data. The purpose of the BMS is to support the functioning of the CIR and the MID. Without a shared BMS, performing biometric matching through the CIR and MID would not be possible. As seen in Table 2, the BMS will store biometric templates in form of fingerprints and facial images[82] from five out of the six existing EU databases:

Yet, the BMS will not be directly accessible. Law enforcement authorities of the Member States will use it by querying the CIR with the biometric data of a person taken during an identity check. It has been already argued above that, to comply with the

79 GDPR, supra n 43 at Article 9(g).

80 See, respectively, Case C-291/12 *Schwarz v Stadt Bochum* [2014] 2 CMLR 5 at para 40; *M.K. v France* Application No 19522/09, Merits and Just Satisfaction, 18 April 2013 at para 40.

81 The ETIAS is the only database that does not gather biometric data.

82 Other biometrics such a palm print data and DNA profiles are not going to be used for the cross-verification as they are only stored in SIS.

data minimisation principle, the consultation of the biometric data stored in the CIR to identify a person during an identity check should only be carried out as a last resort.[83]

However, the Interoperability Regulations are silent on this matter. Certainly, Article 20 of Interoperability Regulation 818 establishes that a police officer can only carry out a query of the CIR if the person 'is unable or refuses to cooperate', but nothing is mentioned on the particular querying of biometric data. For this type of data, conditions must be even more stringent. Ideally, only in cases where a person is not willing to cooperate by providing their documents and identity, or where there is a well-found suspicion that they are false, only then should biometric data in the CIR be queried. In this sense, the EDPS is also rightly concerned that were there to be a data breach or a misuse of data affecting the CIR, a very large number of individuals could have their highly sensitive biometric data exposed.[84]

In addition, it is worrying that the Interoperability Regulations do not provide any specific protection for the processing of biometric templates to be stored in the BMS.[85] Biometric templates are digital representations of the unique features of a biometric sample. They represent the physical characteristics of the biometric collected based upon unique data points that such a biometric has. These points get translated into this mathematical equation, which can be used anytime to reconstruct that particular biometric data that were once collected.

The Commission has claimed that biometric templates are not personal data and, therefore, no further protection is needed.[86] However, it is reasonable to consider biometric templates as personal data since they could eventually make an individual (directly or indirectly) identifiable. This interpretation has been supported by many scholars[87] and also by the Article 29 WP, who noted back in 2003 that 'measures of biometric identification or their digital translation in a template form [are] in most cases [. . .] personal data'.[88] Hence, a specific provision detailing the procedures, limits and data protection rules in relation to on the processing of biometric templates should have been incorporated in the Regulations.

The processing of biometric data is particularly alarming in the case of vulnerable groups of persons, such as refugees and asylum seekers. These groups are particularly prone to demonisation within various sectors of media outlets, making them more vulnerable.[89] The new interoperability system will allow police authorities to send biometric verification of refugees and asylum seekers, information that is today still only accessible by border authorities under the Eurodac system. The Eurodac system was put in place to register fingerprints and complement the *Dublin system* to promptly identify the Member State responsible for asylum requests based on a mechanism assigning

83 EDPS, supra n 52 at 14; Article 29 WP, supra n 65, at 11.

84 EDPS, supra n 52 at 11.

85 Quintel, 'Connecting personal data of Third Country Nationals: Interoperability of EU databases in the light of the CJEU's case law on data retention', 28 February 2018 at 16, available at: www.orbilu.uni.lu/handle/10993/35318 [last accessed 31 March 2020].

86 European Commission Impact assessment, supra n 18.

87 See Jones, supra n. 64 at 22; Gutheil, supra n 15 at 13; Article 29 WP, supra n 65 at 8; Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (2013) at 94–100.

88 Article 29 Data Protection Working Party, Working Document on Biometrics, WP80, 1 August 2003.

89 Massimino, 'The Border and beyond: The National Security Implications of Migration, Refugees, and Asylum under U.S. and International Law' (2018) 9 *Journal of National Security Law & Policy* 659.

the obligation to provide international protection to the country of first entry. Now this purpose has been expanded,[90] allowing the processing of Eurodac data in the fight against the security threat of terrorism and causing the association of asylum seekers' data to criminal records in the EU.

For all that is said above, a solution to reinforce the protection of biometric data would be to change the underlying of BMS to only match data, without storing it. This has been already recommended by the European Agency for Fundamental Rights [91] and by the Article 29 WP.[92] However, for now, the BMS will actually store the biometric templates of fingerprints and facial images, which could infringe Article 9 of the GDPR.

(iii) Doubtful compliance with the necessity principle

Regarding the principle of necessity, it is often assessed when there is a restriction of a fundamental right to the protection of personal data. In the case of the new interoperability components, where there are clear conflicts with the elements of data protection (as previously discussed), its actual creation should therefore be justified based on a clear necessity. The necessity for the new interoperability components has been already criticised because the existing databases are in general functioning well, and no demonstration of major shortcoming or ongoing failures within their technical or operational implementation has been provided. [93] For instance, for the purpose of identification, the existing SIS already uses biometric data for identifying or verifying the identity of third-country nationals on the territory of a Member State. This database works properly, so it is unclear why the existing capabilities for identity checks within the territory of the Member States need to be extended to other existing databases like, for example, EES. [94] One theory is that some of the original purposes of the existing databases have politically failed—namely, the management of migration to the EU—and, therefore, there is a need to reconceptualise some of the existing databases. One of the best examples of this is Eurodac. The failure of the Dublin system[95] may strip away its necessity, and as a result, new broader justification and migration objectives for maintaining and legitimising the instrument could have been created. [96]

The necessity of establishing four new components (the ESP, the BMS, the MID and the CIR) is not clear. They are new elements created for accessing data from all types of third-country nationals. The necessity is especially questionable because this newfound functionality does not prevent law enforcement authorities from obtaining information about individuals without a solid justification. By only introducing one item of personal data (e.g. the name and surname), the ESP will allow law enforcement to learn whether information about a third-country national is stored on one of the existing EU databases. Similarly, a police officer will be able to query the CIR and receive a response in form of a hit/no-hit whenever they deem it convenient. For instance,

90 Probably for the failure of the Dublin system itself, as suggested by Vavoula, supra n 26 at 365.
91 FRA, supra n 70 at 24.
92 Article 29 WP, supra n 65 at 9.
93 Article 29 WP, supra n 65 at 4.
94 Gutheil, supra n 15 at 54.
95 Becker, 'EU "Asylum System"—Elements, Failure and Reform Prospects' in Wacker, Becker, and Crepaz (eds), *Refugees and Forced Migrants in Africa and the EU* (2019) at 37–68.
96 Vavoula, supra n 26 at 365.

by introducing the name of a person, there system may flag a hit saying that there are six extra records on the query. This information will not transmit the details of those six records/pieces of personal information, as full access can only be granted if there is enough proof of need and specificity. Yet, the simple hit-flag already reveals some personal information about the individual *ex ante*, without having to access to their full data (for instance, law enforcement will be able to see whether the individual is a Schengen visa holder or has applied for international protection).[97]

Therefore, as claimed by the EDPS and the Article 29 WP, the processing of such data through a 'hit-flag' constitutes an interference with the fundamental rights as protected by Articles 7 and 8 of the Charter and must comply with Article 52(1) of the Charter in terms of necessity and proportionality.[98] To that end, in *Schrems II*,[99] the CJEU reaffirmed the importance of complying with the fundamental rights of the Charter, even beyond the EU territory. Particularly, on 16 July 2020, the Court invalidated Privacy Shield Decision because the US laws could not ensure a level of protection essentially equivalent to that guaranteed by Articles 7, 8 and 47 of the Charter.[100]

In the same way, this consultation mechanism bypasses the necessity requirement established by the CJEU in *Digital Rights Ireland*[101] and *Watson*.[102] In both cases, the Court concluded that only a court or an independent administrative body can authorise access to data and whether this is strictly necessary for the specific purpose within the framework of procedures of prevention, detection or criminal prosecutions.[103] However, the interoperability components may allow police and border authorities to access certain personal data items without the supervision of a judicial body.

B. Discrimination Against Third-Country Nationals

The Lisbon Treaty includes in Article 10 TFEU a horizontal clause with a view to integrating the fight against discrimination into all EU policies and actions. Likewise, Article 21 of the EU Charter of Fundamental Rights prohibits any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. The Interoperability Regulations contain some anti-discrimination safeguards too.[104] However, these provisions do not take away the discriminatory nature of the system itself,[105] as at least two types of discrimination would take place by law enforcement using the system: (a) discriminations based on ethnic and national origin and (b) discriminations based on race.

97 Gutheil, supra n 15 at 66.
98 EDPS, supra n 52 at 16; Article 29 WP, supra n 65, at 13–14.
99 Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, ECLI:EU:C:2020:559.
100 Ibid. at para 180.
101 *Digital Rights Ireland*, supra n 59.
102 Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, ECLI:EU:C:2016:970.
103 *Digital Rights Ireland*, supra n 59 at para 62; *Watson*, supra n 106 at para 120.
104 Article 5 and Article 20(5) of Interoperability Regulation 818.
105 Meijers Committee, supra n 78 at 3.

Differences based on national origin are in essence the purpose for adopting the Interoperability Regulations, as they incorporate additional security checks for third-country nationals, allowing a differentiated treatment between EU citizens and third-country nationals.[106] The new Regulations place in the same box short-stay travellers, migrants, asylum seekers, irregular migrants and criminals,[107] having only one thing in common: they are third-country nationals. No connection whatsoever to an illegal behaviour will be considered when collecting their data.[108] Thus, this system seems to be based on the (wrong) idea that non-EU nationals are more likely than EU nationals to be engaged in activities threatening public,[109] bringing closer the controversial concept of 'pre-crime'.[110] It certainly creates an unjustified difference of treatment between EU citizens and third-country nationals.

In particular, the CIR can lead to racialised discriminatory policing practices too. When using the CIR for identity checks, there is a risk of systematically stigmatising certain people (or groups of people) based on their race or appearance. For instance, there is no information published in the Regulations detailing the mechanism to ensure that an agent does not select an individual for an identity check solely based on their religion, background or even race (e.g. black people or those from an ethnic group). Although law enforcement agencies often present their technology and systems as 'race' neutral, studies have already proved that the impact of new technologies to identify, monitor and analyse personal information is disproportionately felt by minority ethnic communities who tend to be over-policed and subject to higher levels of background checks.[111] This is in addition to the recent tendency of mistakenly attributing certain offences such as drug dealing, theft, street robbery, religious extremism, radicalisation, street gangs and serious violent crime (e.g. knife crime) as being particular to minority ethnic groups and communities.[112] The over-processing of data from these groups of people through use of the interoperability system may inadvertently help fuel and exacerbate such misconceptions. It is worth highlighting that, by conducting these practices, competent authorities in Member States could be infringing their obligations as enshrined in the EU Charter of Fundamental Rights. In this sense, and in the terms of *Bauer*, [113] individuals should be able to bring actions based directly based on the Charter against Member States in the national courts in the event that they can demonstrate violations of specific rights in the Charter by officials of a Member State.

106 EDPS, supra n 52 at 14; Brouwer, 'Large-Scale Databases and Interoperability in Migration and Border Policies: The Non- Discriminatory Approach of Data Protection' (2020) 26 *European Public Law* 1 at 85.

107 Gutheil, supra n 15 at 52.

108 Meijers Committee, supra n 78 at 3.

109 Nunziata and Luca, 'Immigration and Crime: Evidence from Victimization Data' (2015) [2015] 28 *Journal of Population Economics* 3 at 697–736; Lyons, Vélez and Wayne, 'Neighborhood Immigration, Violence, and City-Level Immigrant Political Opportunities' (2013) 78 *American Sociological Review* 4; Bernat, 'Immigration and Crime' in *Research Encyclopedia of Criminology* (2017).

110 EESC, supra n 34 at 53.

111 Williams and Kind, 'Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices Across Europe' (2019) *European Network Against Racism and Open Society Foundations* at 6, available at: www.statewatch.org/media/documents/news/2019/nov/data-driven-profiling-web-final.pdf [last accessed 7 December 2020].

112 Ibid. at 11.

113 Joined Cases C-569/16 and C-570/16 *Bauer et al. v Broßonn*, ECLI:EU:C:2018:871.

It can be concluded that the Interoperability Regulations not only increase the risk of discrimination on grounds of nationality but are also likely to increase discrimination on the basis of racial or ethnic origin, thereby infringing on the right of non-discrimination described in Article 21 of the EU Charter of Fundamental Rights. If that occurs, individuals who are victims of these discriminating practices could start judicial proceedings against the specific Member State for alleged violation of Article 21 of the Charter. Although ways to avoid discrimination have been proposed,[114] the Interoperability Regulations do not include any preventive mechanism against it.

C. The Processing of Children's Data

The Regulations prohibit sending queries of the CIR for the purposes of identifying minors under the age of 12 years old, unless it is in best interest of the child.[115] Thus, a police or border authority could send a query to the CIR with biometric or alphanumeric data of any person over the age of 12, or even an undocumented minor who they think is over 12.[116] First of all, one could question why 12 years old was chosen as the threshold. The reason lies most probably in the fact that most of the existing EU information systems have similar clauses for children with the same age threshold too.[117] Surprisingly, the proposed VIS proposal lowers the fingerprinting age for children in the visa procedure to 6 years old, [118] which is clearly at odds with the above threshold for the querying of minors. It is arguable that processing data (and even sensitive data) from children over 12 increases their level of protection in case they go missing or get abducted. It is certainly the case that interoperable EU information systems can be a very effective tool for child protection in this sense, as they could help finding missing children. Law Enforcement Agencies involved with abduction or emergency cases often speak of the 'golden hour' immediately following the event where fast access to relevant information is paramount in achieving good outcomes. Today, many children get lost at the border crossing points and, because they have not been previously identified, they may never be found. In cases where a missing child is reported through SIS, there is no alert because SIS is still not connected to other databases. The new interoperability system will thus improve the (albeit inaccurate) data that exist today on missing children. Similarly, one can say that lowering the fingerprinting age for children will strengthen the prevention and fight against children's rights abuses, in particular, by enabling the identification/verification of the identity of third-country national children who are found in Schengen territory in a situation where their rights may be or have been violated (e.g. child victims of human trafficking).

114 Catanzariti, 'Individuals or "Bare Data"? Un-owned Data for Interoperable Borders' (2020) Blog Forum European University Institute, available at: www.migrationpolicycentre.eu/individuals-or-bare-data/ [last accessed 31 March 2020].

115 Interoperability Regulation 818, supra n 1 at recital 28.

116 In this sense, it is not clear how can an authority be certain that a minor is 12 years old and not 11 or 10 if there is no identification card to prove it.

117 See EES Regulation, supra n 17 at Article 10(2); Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 142/1 at Article 1.

118 Council of the European Union, supra n 83 at para 8.

However, it is disturbing that the interoperability system collects data (including biometric data) from minors who are 12 years old and above. It is submitted that the processing of minors' data through the same mechanisms as those of adults contravenes Article 3 of the UN Convention on the Rights of the Child and Article 24 of the EU Charter of Fundamental Rights. According to these laws, children should have dedicated and specific safeguards, protection and care, as necessary for their well-being. to the provisions for the retention of children's data within the system also violate these provisions. In the particular matter of data retention, the ECtHR stated in the *S. and Marper case*[119] that blanket retention of biometric data by law enforcement authorities of persons not convicted of a crime may be especially harmful for children. The court has explained that this retention could be particularly damaging in the case of minors, given their special situation and the importance of their development and integration in the society. A child may indeed suffer great social stigma and psychological implications provoked by the long retention of their personal data, affecting negatively on their motivation to bring a constructive role in society. In the case of migrant children, the implications of retaining their data can be even more damaging due to their double vulnerability, being both migrant and children. Moreover, biometric data of children may entail ongoing logging of quickly obsolete data, as children go through great physical development in very short time, which means that the margin of error for children's data will probably be higher than for adults. Hence, fingerprints and particularly facial data of children are unlikely to be reliable as time passes.

In conclusion, it is unclear whether children will be safeguarded or unprotected through the introduction of the new interoperability components. In any case, in line with the Article 29 WP and EESC recommendations,[120] specific additional protection for children in the context of the CIR, the BMS and the MID are most likely necessary.

D. Violation of the Proportionality Principle

As the CJEU stated back in 1970, the principle of proportionality should be assessed with the consideration that individuals may only have obligations based on the degree strictly necessary for purposes of public interest.[121] Proportionality is thus a general principle of EU law that restricts authorities in the exercise of their powers by requiring them to strike a balance between the means used and the intended aim. The new interoperability legislation calls into question this proportionality.[122] First of all, access to the CIR is permitted for the wide purpose of 'ensuring a high level of security', without precisely prescribing specific offences or legal thresholds that could justify such access. The fact that law enforcement authorities can send queries without specifically defined thresholds implies that non-EU nationals *a priori* constitute a security threat.[123] Although the majority of individuals whose data will be stored in the CIR will surely be *bona fide* third-country travellers, migrants and asylum seekers, their data would

119 *S. and Marper v United Kingdom*, Application No 30562/04 and 30,566/04, Merits and Just Satisfaction, 4 December 2008, at para 124–125.

120 Article 29 WP, supra n 65; EESC, supra n 34 at 53.

121 Joined Opinion of Mr Advocate General Dutheillet de Lamothe in Cases 11–70, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, Reference for a preliminary ruling: Verwaltungsgericht Frankfurt am Main—Germany, 2 December 1970.

122 Article 29 WP, supra n 65 at 6; Quintel, supra n 88 at 16.FRA, supra n 70 at 36–37.

123 EDPS, supra n 52 at 14.

be stored side by side with convicted criminals (from ECRIS-TCN).[124] The proportionality principle is thus infringed since there is no concrete definition of the offences that should permit police/border authorities to access personal data within the system. In fact, the Commission is already considering limiting the access of ECRIS-TCN data to the most serious offences, namely, 'terrorist and serious criminal' offences.[125] Otherwise, it would permit, if not encourage, authorised authorities to use the CIR to tracking records of minor offences and for any other reason which could be claimed to be part of the broad security purpose. It can be thus concluded that the principle of proportionality is not sufficiently justified in the Interoperability Regulations. In this sense, further provisions must be been added to ensure that the new systems are not abused in the application of the 'ensuring a high level of security' purpose.

6. CONCLUSIONS

The preference towards the fragmentation of the EU information systems has been maintained for many years. Whilst this fragmentation may have been by necessity rather than by design, this formula has served to preserve fundamental rights such as the right to privacy and data protection, by keeping the purpose and scope of each tool clearly specified. Now the EU has shifted its view, favouring the creation of a centralised interoperability scheme that collects and shares information about the millions of third-country nationals seeking to enter the EU. The reason given for this change is fundamentally that a better connection amongst exiting EU information systems will create homogeneity across the Member States, allowing more uniform application of security, migration and asylum management in the EU.

However, the new interoperability components are likely to result in violations to fundamental rights, such as the right to privacy and data protection, the protection of the child, the non-discrimination principle and the principle of proportionality. Particularly, regarding the right to privacy and data protection, this article has demonstrated how the interoperability components open questions regarding the compliance with the purpose limitation principle, the principle of fairness and transparency, the data minimisation principle, the data accuracy principle and the data storage limitation.

The EU has clearly become a 'Security Union' by prioritising collective security over individual fundamental rights. By blurring the boundaries between immigration and criminal law, this also confuses the distinction between terrorists, criminals and foreigners. Unfortunately, this approach lowers considerably the safeguards for third-country nationals, who include asylum seekers and the most vulnerable of migrants, who are thus deprived of their basic human rights as enshrined in the EU laws and the EU Charter of Fundamental Rights.

124 Article 29 WP, supra n 65 at 7.

125 European Commission (2019), Analysis of the Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) 2019/816 1, and of the Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) no 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/18612, Directorate-General for Migration and Home Affairs at 16.

ACKNOWLEDGEMENTS

The author is grateful to Christopher Neeson and to the anonymous reviewer for their feedback on earlier drafts of this article. This study is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 882986.