Market and Competition Law Review / VOLUME III / No. 1 / APRIL 2019

The Impact of EURODAC in EU Migration Law: The Era of *Crimmigration*?*

*Benedita Menezes Queiroz***

ABSTRACT: Counter-terrorism and public security measures have significantly altered EU immigration law. Under the premise that EU instruments which regulate EU immigration databases influence the legal regime of irregularity of migrants' statuses, the present article argues that the latest developments in the area of data technology contribute to the phenomenon of "crimmigration". This is so not only because they may generate a sort of "digital illegality" due to their impact on the categorisation of migrants, but also because they enable a conflation of treatment of irregularity, asylum seeking and criminality. This article focuses on the recent amendments and proposals for amendments to the EURODAC Regulation, a database that regulates the asylum fingerprint system in the EU. This is revealing of the ongoing broadening of the purpose of that data and law enforcement access to the collected information. The argument finds its basis in three main trends common to these databases: the erosion of the principle of purpose limitation, the widening of access to data by law enforcement authorities, and the digitalisation of borders through biometrics. Ultimately, this article claims that the level of surveillance of certain categories of migrants that may cross the borders of the EU puts at risk the distinction between illegally staying irregular migrants and criminals, given that the treatment of their personal data is insufficiently clear in practice.

KEYWORDS: EURODAC, asylum seekers; illegally staying third-country nationals; immigration databases; crimmigration; surveillance; digital borders.

---

* Date of Reception: 30 December 2018. Date of Acceptance: 17 January 2019.

** Porto, Portugal, bmqueiroz@porto.ucp.pt (Guest Assistant Professor, Universidade Católica Portuguesa, Escola de Direito Porto and Teaching Assistant, School of Transnational Governance, European University Institute, Italy).

1. Introduction

The so-called EU migration crisis came to prominence in 2014 and 2015 due to conflict and violence in a number of different countries including Syria, Afghanistan and Iraq. A mass influx of refugees arrived at the shores of the European Union (in 2015 one million asylum seekers)[1] and these events prompted the EU Commission to develop a European Agenda on Migration aimed at addressing the challenges that Europe was facing at the time (and is still facing today, although the numbers are not as high as they were at the peak of this crisis). Efficient border management through better use of IT systems and technologies was one of the top policy priorities for the Commission at this stage. By making full use of these systems the EU wanted not only to improve border management, but also to reduce irregular migration and return illegally staying third-country nationals.

First and foremost, borders are a form of expression of a State's sovereignty. In the EU, borders have been gradually allocated new tasks after the implementation of the information exchange systems in the Area of Freedom, Security and Justice (hereafter AFJS) since the SIS in 1995. These new tasks are related primarily to the categorisation of migrants who want to enter the EU and migration governance. Furthermore, the introduction of information technology has also contributed to the "transformation of European borders to digital borders",[2] a process that is at the heart of the present study.

EU databases play a crucial role in the categorisation of migrants in Europe. The registration of people in EU databases and the storing of their fingerprints or other types of personal data catalogue those arriving in EU territory.[3] However, the role of EU information systems is not limited to the collection of personal information on mobile third-country nationals. It also influences EU policy options that impact migration governance overall and migrants' rights. The most recent modifications and proposals in the area of EU immigration databases have amplified their functions,

---

[1] Alexander Betts and Paul Collier, *Refuge – Transforming a Broken Refugee System* (London: Penguin Books, 2017), 2.

[2] Michiel Besters and Frans WA Brom, "Greedy information technology: The digitalization of the European migration policy", *European Journal of Migration and Law* 12 (2010): 456, and Louise Amoore, "Biometric borders: Governing mobilities in the war on terror", *Political Geography* 25 (2006): 336.

[3] Dennis Broeders, "A European 'border' surveillance system under construction", in Dijstelbloem Hubb and Meijer Albert (eds.), *Migration and the New Technological Borders of Europe. Migration, Minorities and Citizenship* (London: Palgrave Macmillan, 2011), 43.

enlarged their purposes and increased the number of authorities with access to them (for instance as we will see in relation to EURODAC) for the purposes of fighting against terrorism and combatting serious crime. Such developments reflect EU's concern in addressing the terrorist threat and enhancing security within the European territory through data surveillance. Nevertheless, these initiatives have also brought problems with regard to the accuracy in the use of biometrics,[4] the possibility of conflating asylum seeking with potential suspicion of crime, the erosion of the purpose limitation principle and in some cases unauthorised access to the databases.

Four centralised, large-scale EU databases must be mentioned in relation to the exchange of personal information of third-country nationals (and EU citizens in a lesser extent): a) the SIS/SIS II (Schengen Information System and the Second Generation Schengen Information System); b) the VIS (Visa Information System); c) EURODAC (European Dactylographic System); and d) EES (Entry Exit System), adopted in 2017 but operational only from 2020 (hereafter EES).

This study questions whether the development of EU databases in the AFJS, in particular EURODAC, could lead to questioning the lawfulness and proportionality of the further use of these databases.[5] What is central is a reflection on how the latest developments in the area of AFJS databases influence the categorisation of migrants under EU law, in particular asylum seekers. If European borders are "being transformed into digital borders",[6] how does this digitalisation of borders affect asylum seekers' and irregular migrants' statuses in the European Union?

In recent years there has been a significant increase in the personal data stored by these information databases, relating more and more to crime and law enforcement issues. The combination of the latter trends with broader access of law enforcement authorities to these information systems has contributed considerably to transforming their primary purposes. By carefully analysing how the change in their purpose has affected the

---

[4] Approximately 5% of the world population does not have fingerprints or their fingerprints are not readable by a machine, especially children and elderly people.

[5] Evelien Renate Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, vol. 15 (Leyden: Brill, 2008), 144.

[6] Besters and Brom, "Greedy information technology: The digitalization of the European migration policy", 455.

European migration regulation, it is argued that the "digital explosion"[7] plays a momentous role. The following aspects must be taken into account throughout the analysis of EURODAC and its impact in EU Migration Law:

(i) The erosion of the purpose limitation principle;
(ii) Enhanced accessibility by law enforcement authorities to EU immigration databases;
(iii) The digitalisation of borders through biometrics.

2. EURODAC and the Common European Asylum System

The EURODAC was established by Council Regulation 2725/2000 (hereinafter EURODAC Regulation).[8] This database, which became operational in January 2003, was designed to assist in the determination of which Member State is responsible for examining an asylum claim lodged in a Member State, in accordance with the conditions set out in the Dublin Regulation.[9] The Dublin Regulation aims to prevent so-called "asylum shopping",[10] and the EURODAC Regulation determines whether an individual has already sought sanctuary in another Member State. The UK and Ireland chose to be part of this Regulation that develops part of the Schengen *Acquis*; similarly, Denmark and the Schengen Associated Countries are covered by the Dublin Regulation and EURODAC.[11] Both the EURODAC Regulation and the amended Dublin Regulation (hereinafter Dublin III Regulation) are closely intertwined due to the fact that EURODAC is crucial for the

---

[7] Hal Abelson, Ken Ledeen and Harry R Lewis, *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion* (Addison-Wesley Professional, 2008).

[8] Article 1 (1) of the Council Regulation (EC) No. 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, [2000], OJ L 316/1. This Regulation became operational in 2003 (hereafter EURODAC Regulation).

[9] *Ibid*., Recitals 2 and 3.

[10] Asylum shopping can be one of two situations. Firstly, the abusive practice of claiming asylum in more than one Member State and, secondly, the "comparison and selection of one asylum rule among several". All in all it is when asylum seekers apply for asylum in more than one EU State or choose one EU State in preference to others on the basis of a perceived higher standard of reception condition. For a more comprehensive note on the second meaning of "asylum shopping": Ségolène Barbou des Places, "Evolution of asylum legislation in the EU: Insights from regulatory competition theory", *RSCAS Working Paper* 16 (2003), 3-7.

[11] Jorrit Rijpma, *Building borders: The regulatory framework for the management of the external borders of the European Union*, PhD dissertation, European University Institute, Florence, 2009, 201. However, in the recast, Ireland chose not to be part of the EURODAC II Regulation.

functioning of the Dublin regime.[12] As such, the two Regulations were amended together in June 2013.[13]

The EURODAC II Regulation entered into force on 19 July 2013 and was applicable from 20 July 2015 onwards.[14] Currently, the EURODAC information system may collect and store fingerprints of three categories of migrants: applicants for international protection, migrants who have crossed the borders of the EU irregularly and are arrested, and migrants who have been found illegally staying within EU territory.[15] Some scholars such as Brouwer have criticised the inclusion of illegally staying migrants in the EURODAC database system, highlighting the fact that fingerprinting illegally staying migrants is potentially problematic.[16] The author argues that the inclusion of categories two and three of migrants is "unacceptably large" due to the fact that since these persons have not applied for asylum it is difficult to justify how the Dublin Convention can substantiate such fingerprinting. Under the EURODAC Regulation, which specifically lists law enforcement as one of its objectives, this objection could in part be refuted. Nevertheless, one may not refute it completely given that, for example, it allows Member States' designated authorities to compare Europol fingerprints collected by EURODAC with those linked with criminal investigations for law enforcement purposes.[17] This measure reflects the erosion of the purpose limitation principle, but may also consequently contribute to a discriminatory treatment of asylum seekers by associating

---

[12] European Parliament and Council Regulation (EU) No. 603/2013 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 (recast), [2013], OJ 2013, L 180/1 (hereafter EURODAC Regulation II).

[13] European Parliament and Council Regulation (EU) No. 604/2013 of the 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 (recast), [2013], OJ 2013, L 180/31.

[14] Article 46 of the EURODAC II Regulation.

[15] *Ibid*., Articles 9 (1) and 14 (1).

[16] Evelien Renate Brouwer, "Eurodac: Its limitations and temptations", *European Journal of Migration and Law* 4 (2002): 236.

[17] Article 7 (2) of the EURODAC II Regulation.

them with criminals, which are aspects that will be addressed in further detail in the sections below.

As a consequence of the mass influx of refugees in Europe in 2015, frontline Member States like Greece and Italy faced numerous challenges including difficulties with fingerprinting all of those arriving irregularly at the EU, which led to thousands of migrants left without registration. The European Commission presented, in May 2016, a proposal for another recast EURODAC Regulation.[18] This proposal was part of a package of measures that aimed to reform the Common European Asylum System. The main purpose of the 2016 recast EURODAC Regulation proposal was to mirror the changes in the proposed reform of the legal framework of the Common European Asylum System presented in May 2016.[19] Among other measures, the EU Commission proposed the use of more biometric identifiers for EURODAC, for example, facial recognition, collection of digital photos and extension of the scope of this database.

Although the 2016 proposal for recasting the EURODAC Regulation is still at the EU negotiation table, it reflects the continuous expansion of EURODAC's purpose and scope, an aspect that makes some authors question the substantive legality of this database.[20]

3. EURODAC and the erosion of the purpose limitation principle

Purpose limitation is a core principle of data protection law and applies to national and international rules concerning data. Article 5 of the Council Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data helps us understand the meaning of this principle by establishing that data automatically processed shall be: "a)

---

[18] Proposal for an European Parliament and Council Regulation (EU) No. 2016/0132 of 4 April 2016 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) (hereinafter Proposal 2016 recast EURODAC Regulation).

[19] The Commission's reform of the Common European Asylum System includes three proposals: a) amending the Dublin Regulation, b) creating the European Agency for Asylum and the c) reform of Eurodac system.

[20] Valeria Ferraris, "Economic Migrants and Asylum Seekers in Ten Fingers: Some Reflections on Eurodac and Border Control", 2017, https://www.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2017/05/economic-migrants.

Obtained and processed fairly and lawfully, b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes, c) adequate, relevant and not excessive in relation to the purposes for which they are stored, d) preserved in a form which permits identification of data subjects for no longer than is required for the purpose for which those data are stored".[21]

The purpose limitation principle was subsequently included in Article 6(1) (b) of Directive 95/46,[22] which once again set out that personal data should be acquired for specified, explicit and justified purposes. Furthermore, such data should not be processed in any way incompatible with these purposes. Article 5 b) of the General Data Protection Regulation of 2016,[23] repealing Directive 95/46, states 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". As such, data must only be used for legitimate purposes, equivalent to a "ban on aimless data collection".[24] Additionally, these legitimate purposes must be specified before collection, and use or disclosure of the data must be compatible with the specified purposes. Finally, the principle of purpose limitation entails that data should not be retained for any period longer than necessary with regard to the purposes for which it was collected and stored.

Related developments include new information technology, biometric data beginning to be used and the creation of multipurpose, large-scale databases. At the same time, data protection has been recognised as a human right in accordance with Article 8 of the Charter on Fundamental Rights of the EU (hereinafter the Charter) and Article 8 of the European

---

[21] Article 5 of the Data Protection Convention.

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

[23] European Parliament and Council Regulation (EU) No. 679/2016 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 2016, L 119/1.

[24] Article 5 (1) b) of the General Data Protection Regulation; Evelien Renate Brouwer, "Legality and data protection law: The forgotten purpose of purpose limitation", in Leonard F. M. Besselink, Frans Pennings, and Sacha Prechal (eds.), *The Eclipse of the Legality Principle in the European Unio*n (Alphen aan den Rijn: Kluwer Law International, 2011), 275, designation used by Brouwer when referring to the prohibition of collecting and storing personal data for unknown or not specific purposes.

Convention of Human Rights (hereinafter ECHR).[25] According to certain commentators, three objectives are key to the right to data protection, namely the protection of individual rights,[26] the protection of the rule of law,[27] and the protection of "good governance".[28]

Taking EURODAC as an example, given that it is the focus of the present study, this database was created neither to fight irregular migration nor to identify an illegal stay. Rather, EURODAC is an immigration database created to support the implementation of EU asylum policy and to perform mainly administrative tasks to guarantee the effectiveness of the Dublin System, as mentioned above. EURODAC's original purpose of facilitating the application of the Dublin Convention was set out in the first version of the EURODAC Regulation.[29] This formulation was retained in the amended EURODAC Regulation, although point 2 added to Article 1 EURODAC II Regulation expanded the purpose of the regulation.[30] This provision raised significant concerns, not only with regard to changing the original core purpose of that information system, but also to migrants' fundamental rights.[31] As such, Article 1 (2) EURODAC II Regulation significantly affects the accessibility of EURODAC – expanding the number of bodies which have access to the biometric database that stores fingerprints for 18 months[32] or 10 years.[33] Consequently, this amendment formalises the extension of the scope of EURODAC for law enforcement purposes, which is made clear from the wording of Recitals 7, 8 and 9.[34]

---

[25] Article 8 of the ECHR and Article 8 of the Charter on Fundamental Rights of the EU.

[26] Brouwer, "Legality and data protection law: The forgotten purpose of purpose limitation", 275.

[27] See the Preamble of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, [1981], (hereafter Data Protection Convention).

[28] Brouwer, "Legality and data protection law: the forgotten purpose of purpose limitation", 275.

[29] Article 1 (1) of the EURODAC I Regulation.

[30] The accessibility clause, as for the purposes of this chapter, is analysed below in the next subsection.

[31] European Data Protection Supervisor, European Data Protection Supervisor Press Release, EDPS/12/12 – "EURODAC: Erosion of fundamental rights creeps along", Brussels, 5 September (2012).

[32] Article 16 of the EURODAC II Regulation.

[33] Article 12 of the Proposal 2016 recast EURODAC Regulation.

[34] Since 2007 the Commission alerted for the fact that the future developments of this database would probably focus on the use of the data for law enforcement purposes in the Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, COM 299 final and SEC 742, [2007], 11.

It is questionable whether the more recent regulation represents a form of "function creep", as some have argued.[35] As one commentator has stated, function creep happens when "the system is being stretched in order to fulfil an increasing number of different types of functions than those for which it was originally created".[36] To take one example, personal data such as fingerprints stored for one specific objective might subsequently be made available for other purposes, such as for investigative police work. Moreover, an extension scope of EURODAC was recently put forward by the EU Commission in the 2016 recast EURODAC Regulation by including the purpose of controlling "illegal immigration and secondary movements within the Union and with the identification of illegally staying third-country nationals for determining the appropriate measures to be taken by Member States, including removal and repatriation of persons residing without authorisation".[37] In addition, the 2016 proposal allows Member States' designated authorities and the Europol to request the comparison of fingerprints and facial image data stored in the Central System for law enforcement purposes "for the prevention, detection or investigation of terrorist offences or other criminal offences".[38]

The erosion of the purpose limitation principle, as demonstrated in the recent shift in the purposes and extension of scope of immigration databases and, in particular, EURODAC, is central to the argument that the asylum seeking and irregularity of a migrant's stay (an immigration law concept) and criminality (a criminal law concept) are increasingly entangled in EU law and at the domestic level.[39]

3.1. Law enforcement authorities' and Europol's access to EURODAC

The topic of the access to personal data stored in the immigration control information systems is directly related with the erosion of the purpose limitation principle addressed above, and deserves being analysed by itself. As one commentator has remarked, "the intertwinement of crime

---

[35] Besters and Brom, "Greedy information technology: The digitalization of the European migration policy", 465.

[36] Broeders, "A European 'Border' Surveillance System", 55.

[37] Article 1 (b) of the Proposal 2016 recast EURODAC Regulation.

[38] *Ibid*., Article 1 c).

[39] For a US perspective on the phenomenon, see Stumpf, "The crimmigration crisis: Immigrants, crime, & sovereign power", 386.

control and migration control" is the definition of *crimmigration*,[40] and the widening of the access to EURODAC to law enforcement authorities is an example of a measure that contributes to that phenomenon.

Concerns with the proportionality and necessity of these measures have also been raised by the European Data Protection Supervisor (hereafter EDPS) and in the literature.[41] The expansion of the access to EURODAC to law enforcement authorities is, on the one hand, the most relevant example of the extension of purpose of this database, and, on the other hand, supports this idea of instrumentalisation of the database for police control purposes. A result of the growing "surveillance society"[42] is how the trust placed in recent technological developments affects the "outline and development of the European migration" discourse.[43]

When first adopted, the Regulation creating EURODAC did not contemplate police access or law enforcement purposes; the fingerprints that were collected for that database were for the sole purpose of determining which Member State was responsible for examining an asylum application. Despite the fact that EURODAC had more of a technical or administrative aim (namely facilitating the application of the Dublin Convention) since 2007 the Commission, stated that the development of EURODAC would result in the "use of data for law enforcement purposes".[44]

The Commission's motivation to this expansion of the access to EURODAC to law enforcement authorities is explained by the need to strengthen security in the EU due to terrorist attacks and threats and to make the Common European Asylum System more efficient. Although national law enforcement authorities' access was only granted with the 2015 amendments to EURODAC, since its creation there were several

---

[40] Joanne van der Leun, Maartje van der Woude, "A reflection on crimmigration in the Netherlands", in Maria João Guia, Maartje van der Woude and Joanne van der Leun (eds.), *Social Control and Justice – Crimmigration in the Age of Fear* (Hague: Eleven International Publishing, 2013), 43.

[41] See for example: Brouwer, "Legality and data protection law: The forgotten purpose of purpose limitation".

[42] Maria Tzanou, *The added value of data protection as a fundamental right in the EU legal order in the context of law enforcement,* PhD dissertation, European University Institute, Florence, 2012.

[43] Besters and Brom, "Greedy information technology: The digitalization of the European migration policy", 457.

[44] Commission of the European Communities, *Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, COM 299 final and SEC 742*, June 6, 2007, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52007DC0299.

proposals put forward aiming at the extension of the use of this database.[45] The Commission argued that enabling law enforcement authorities' access to EURODAC data was in line with the prevention, detection and investigation of terrorism and other criminal offenses which were a priority put forward by the Hague Programme[46] and would guarantee a balanced deal during the negotiations on the reforms of the Common European Asylum System. In the 2009 Impact Assessment, the EU Commission argued that the national and European system dealing with the collection of information on asylum seekers was inefficient and that widening access to EURODAC would be an important measure to contribute to the prevention, detection and investigation of serious crimes by law enforcement authorities.[47] Nevertheless, the Commission also highlighted at the time that, even though the involvement of asylum seekers in crime and terrorist activities was not significant in numbers, due to the important nature of these crimes their impact would be very relevant and, as such, access of law enforcement authorities to EURODAC would be justifiable. The 2012 proposal for the amendment of EURODAC was not accompanied by another Impact Assessment on the topic of the access of law enforcement authorities and the Commission's proposal was based on the 2009 Impact Assessment.

The EDPS pointed out the crucial point: that granting law enforcement authorities access to EURODAC has potentially problematic consequences, namely with regard to the fact that "the necessity of the intrusion must be supported by clear and undeniable elements, and the proportionality of the processing of personal data must be demonstrated", despite the legitimate exceptions to the fundamental rights to privacy and data protection.[48] Simply put, using a database such as EURODAC for a different

---

[45] See, for example, the HL Select Committee on the European Union 40th Report (HL Paper 2005-06).

[46] Commission, *Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes*, COM (2009) 344, September 10, 2009, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52009PC0344, Preamble 2 and Article 1.

[47] Article 13 of the Impact Assessment (2009), *Commission Staff Working Document accompanying the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of EURODAC and to the proposal for a Council decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes*, SEC(2009) 936, 10.9.2009.

[48] European Data Protection Supervisor Press Release, EDPS/09/11, Law enforcement access to EURODAC: EDPS expresses serious doubts about the legitimacy and necessity of proposed measures, Brussels, 8 of October 2009.

purpose than it was originally designed may significantly assist in the fight against terrorism and crime as an investigative tool. However, it may also violate not only the principle of purpose limitation but also the legitimacy of the data processing. The EDPS has additionally questioned whether law enforcement access is necessary in the first place and has argued that the Commission has not shown any substantive reasons for it.[49]

Nevertheless, the EURODAC II Regulation currently allows access to EURODAC collected data by Member States' designated authorities and the Europol for law enforcement purposes.[50] The amendment to Article 1 of the EURODAC Regulation is where this inclusion can be found and, for the purposes of this study, will be labelled as the accessibility clause. The accessibility clause states that under specific conditions "Member States' designated authorities and the Europol may request the comparison of fingerprint data for law enforcement purposes".[51] This amendment to EURODAC concerns for the possible violation of the principle of purpose limitation and the principle of proportionality – an issue to which we shall return. However, before addressing that debate, a clarification on the relationship between the principle of purpose limitation and the EURODAC II Regulation's accessibility clause is required. In reality, this relationship is straightforward since the amendment of the EURODAC II Regulation. Concerns with the violation of the principle of purpose limitation were, at least in part (from a purely formal perspective), allayed when the Regulation expressly formalised the change of the original purpose

[49] Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of Regulation (EC) No. (.../...) (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 the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, OJ C 92/1, 2010, 40.

[50] European Commission amended proposal for Regulation of the European Parliament and of the Council (COM (2012) 254 final), on the establishment of "EURODAC" for the comparison of fingerprints for the effective application of Regulation (EU) No. [.../...] (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 to request comparisons 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, Brussels, 2012.

[51] Article 1(2) of the EURODAC II Regulation.

of EURODAC.[52] As such, it is now expressly recognised that EURODAC lays down the conditions under which Member States' designated authorities and the Europol may request the comparison of fingerprint data with those stored in EURODAC for law enforcement purposes under certain conditions explained below.[53]

Yet, the fact that law enforcement authorities and Europol may have wide access to asylum seekers' fingerprints through EURODAC raises concerns, as it will be shown below.[54] Concerns arise not only with regard to the protection of personal data but also respecting the discriminatory impact of these measures. Is it acceptable to impose a greater level of surveillance on anyone subjected to EURODAC than on other migrants within the population?

3.1.1. Proportionality, necessity concerns and the access to EURODAC by law enforcement authorities

Firstly, it is important to note that the rights protected by the principle of purpose limitation in relation to the collection of biometric information, such as Article 8 ECHR, may allow some exceptions if the collection of that data is legitimate, proportionate and necessary in a democratic society.[55] The widespread access of law enforcement authorities to immigration databases may constitute an exception and in the case of EURODAC, for instance, should be in "accordance with the law", "formulated with precision", "necessary in a democratic society to protect legitimate and proportionate aim and proportionate to the legitimate objective aims to achieve".[56]

In the *S. & Marper v. United Kingdom* case,[57] the European Court of Human Rights (ECtHR) took a particular stance regarding the limits of the collection and protection of biometrical data. In this case, the ECtHR found that the applicants were subjected to discriminatory treatment and a disproportionate restriction on their right to privacy. The applicants, Mr. S and Mr. Marper, were suspected of having committed a criminal offence

---

[52] Recital 13 of the EURODAC II Regulation.

[53] Recital 13 and Article 1 (2) of the EURODAC II Regulation.

[54] See Article 1 (2) of the EURODAC II Regulation.

[55] Article 8 (2) ECHR.

[56] Recital 13 of the EURODAC II Regulation.

[57] *S & Marper v. United Kingdom*, ECtHR (2008) ECHR 1581, (2008) 158 NLJ 1755, (2009) 48 EHRR 50, 25 BHRC 557, [2009] Crim LR 355, Appl. no. 30562/04, 30566/04, judgment of 4 December 2008, paragraph 127 and see also Articles 8 and 14 ECHR.

and had their fingerprints and DNA collected, although they were never convicted of any such crime. The applicants had attempted to secure the destruction of the samples of data but had had their requests refused by UK national authorities. In this particular case, the ECtHR made a crucial point in order to understand the significance of this type of data and its potential effects. The Court confirmed that biometric data contains unique information about the individual capable of affecting their private life.[58] As such, the European Court of Human Rights sought to assess whether the restriction on the applicants' right to privacy was i) in accordance with law, ii) had a legitimate aim, and iii) was necessary in a democratic society. The Court found that it was not acceptable and that "the nature of the powers of retention of the fingerprints, cellular samples and DNA of persons suspected but not convicted of offences"[59] was discriminatory. As a result, the retention of Mr. S and Mr. Marper's personal data constituted an interference with their right to respect for private life.

Comparing the reasoning in this decision with the enhancement of the access to EURODAC by law enforcement authorities, it would appear that standards were not taken into account. Essentially, an asylum seeker who has entered the EU and lodged a claim would have to allow the collection and retention of their biometric data and its access to law enforcement authorities independently of the fact of having or not been convicted for committing a crime.[60] This feature, effectively, brings together asylum seeking, potential illegality (if the claim is refused or if the individual is an irregular migrant stopped at the border) and criminality; this is a conflation that by itself raises questions of proportionality, necessity and non-discrimination.

Additionally, the debate regarding restriction of purpose limitation has already been the topic of discussion in the *Huber v. Germany* case before the CJEU.[61] The first case dealt with the interpretation of the Data Protection Directive 95/46 EC and the second with the relationship between the

---

[58] *Ibid*., paragraph 84, emphasis added.

[59] *Ibid*., paragraph 127.

[60] Opinion of the European Data Protection Supervisor on the amended 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. [.../...] [...] (Recast version), 2012, point 38.

[61] Judgment of 16 December 2008, *Huber v. Germany*, C-524/06, EU:C:2008:724 and Judgment of 20 May 2003, *Rechnungshof v. Österreichischer Rundfunk and Others* C-465/00, C-138/01, C-139/01, EU:C:2003:294.

principle of purpose limitation and non-discrimination. These cases are important benchmarks of the jurisprudence of the CJEU in relation to the regulation of individuals' personal data and are helpful counter examples with regard to what has been said about the latest widening of the access to immigration databases.

As an EU citizen exercising his right of free movement, Mr. Huber considered that such collection and retention of personal data was in violation of Article 18 TFEU prohibiting the discrimination of EU citizens and Directive 2004/38 on the free movement of EU citizens and their family members. Three questions were referred to the CJEU by the German administrative court. The first question concerned the processing of personal data for the purposes of the application of the legislation relating to the right of residence, and the second for statistical purposes. Whereas the Court considered that the collection and retention of such data was necessary for the purposes of contributing to a more effective application of the legislation as regards the right to reside,[62] it decided the opposite and declared that in relation to the statistical purposes claim the necessity requirement was not met. The third question is the most relevant for this analysis, as it concerned the storage of personal data relating to EU citizens for the purposes of fighting crime. The CJEU held that in this case there was a violation of the principle of non-discrimination posited in Article 18 TFEU. For the Court, in a Member State, "the situation of its nationals cannot, as regards the objective of fighting crime, be different from that of Union citizens who are nationals of the Member State and who are resident in its territory".[63]

The *Huber v. Germany* decision plays an important role in understanding, even if by analogy, the potential discriminatory effects that processing data for different purposes may have on the individuals monitored.[64] If, in the words of the Court, there is discriminatory treatment of individuals, if the "difference of the treatment arises by virtue of the systemic processing of personal data relating only to Union citizens who are not nationals of the Member State concerned for the purposes of fighting crime",[65]

---

[62] Judgment of 16 December 2008, *Huber v. Germany*, C-524/06, EU:C:2008:724, paragraph 62.

[63] Judgment of 16 December 2008, *Huber v. Germany*, C-524/06, EU:C:2008:724, paragraph 79.

[64] Joanna Parkin, "The difficult road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law", *CEPS Liberty and Security in Europe* 29 (2011).

[65] Paragraph 80 of the *Huber* judgment.

could we say that by analogy the same effect may occur with regard to third-country nationals? Although the decision under analysis focused on the processing of personal data of EU citizens and not specifically on third-country nationals, the core aspect of the analogy is not the category of people these migrants may belong to, but rather the fact that in these two scenarios a group of people is treated unequally with regard to the processing of personal data that allows the creation of connection with the practice of criminal activities.

In other words, the "unpleasant shadow" mentioned by Advocate-General Poiares Maduro in his Opinion "perpetuates the distinction between 'us' – the natives – and 'them' – the foreigners",[66] and the same thing could by analogy be said about the monitoring of asylum seekers for law enforcement purposes. In practical terms, if an information system that treats EU citizens differently in respect of their nationality for the purposes of fighting crime can potentially have stigmatising effects, then the fact that different categories of third-country nationals may be registered in different databases (with or without law enforcement, depending on their origin or claim) can arguably also have the same effects.[67] For instance, as regards EURODAC, one may question whether there is an implicit differential treatment imposed on asylum seekers and irregular migrants registered on that database and other categories of migrants. These are issues that raise concerns in what respects the necessity of different treatment and the proportionality of these measures when there is no strong link between a specific group of people and crime.

In short, a database like EURODAC, which was originally created with an administrative purpose, may in practice work as an intelligence tool,[68] raising concerns with regard to the proportionality and necessity of the means used to achieve the aim proposed. These proportionality and necessity concerns are, for instance, balanced by the conditions imposed by the EURODAC Regulation II to law enforcement authorities to access the information storage by the database. These conditions aim at guaranteeing the protection of the fundamental right to respect for the private life of individuals whose personal data is collected by EURODAC.

---

[66] Opinion of Advocate General Poiares Maduro delivered on 3 April 2008, *Huber v. Germany*, C-524/06, EU:C:2008:194, paragraph 15.

[67] For example someone registered in EURODAC and someone not registered in that database.

[68] Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, 292.

Firstly, and before requesting access to EURODAC data, the designated national authorities must review the national fingerprint databases, the automated fingerprinting identification systems of all other Member States under Decision 2008/615/JHA, and VIS.[69] Secondly, the comparison must be "necessary for the purpose of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, which means that there is an overriding public security concern which makes the searching of the database proportionate".[70] Europol's conditions for access to EURODAC are considerably looser and for instance there is no request for a first check of other databases before Europol's designated authority submits a reasoned electronic request for the comparison of fingerprint data with the data stored in the Central System.[71] In addition to these and to the requirements for the quality of the data,[72] other data protection safeguards are established by the EURODAC Regulation II, such as, for example, the supervision of the data protection being carried out by the EDPS and the national law enforcement authorities.

The trend of the enhancement of the access of law enforcement authorities to immigration databases is a reality confirmed by the EURODAC Regulation II and reaffirmed by the changes put forward by the EU Commission in the 2016 recast EURODAC Regulation, which would, for example, allow law enforcement authorities to check on migrants' secondary movements in the EU's territory or give partial access to the authorities of third countries subject to certain conditions. The Council of the European Union has argued during the negotiations of the 2016 recast EURODAC Regulation that a "broader and simpler access of law enforcement authorities of the Member States to Eurodac may, while guaranteeing the full respect of the fundamental rights, enable Member States to use all existing tools to ensure that people live in an area of freedom, security and justice".[73] Expanding the scope and simplifying law enforcement

---

[69] Article 20 of the EURODAC II Regulation.

[70] *Ibid*.

[71] *Ibid*., Article 21.

[72] *Ibid*., Articles 23 to 25.

[73] Council of the European Union, 10079/17, *Proposal for a Regulation of the European Parliament and of the Council on the establishment of "Eurodac" for the comparison of biometric data 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*

access to EURODAC is, for EU institutions, a tool to "help Member States dealing with the increasingly complicated operational situations and cases involving cross-border crimes and terrorism with direct impact on the security situation in the EU".[74]

The necessity to maintain security in Europe and to overcome the gaps in the registration of asylum seekers and migrants (in particular difficulties with fingerprinting) revealed since the mass influx of migrants to the European Union in 2015 motivated the amendments for the expansion of the scope of and access to EURODAC. Nevertheless, the concerns with the violation of data protection, privacy and discrimination of asylum seekers and irregular migrants are also tangible, despite the safeguards that the EURODAC system imposes, since with broader access to the stored data comes greater responsibility to the designated law enforcement authorities in avoiding this group of migrants being treated as potential lawbreakers.

3.2. EURODAC: biometric borders?

EURODAC's biometric system currently collects ten fingerprints from asylum seekers and migrants aged 14 and older (the 2016 recast EURODAC Regulation proposal suggests lowering the age to 6 years old).[75] The data collected includes fingerprint data, Member State of origin, place and date of the application for international protection, gender, date on which the fingerprints were taken, and the reference number used by the Member State of origin, among other aspects.[76] Therefore, in accordance with the current regime, the individual's name or place of birth is not collected; however, it is possible to link the information stored in the system to a person due to the reference number used by the Member State of origin. The 2016 recast EURODAC Regulation proposal puts forward the possibility of storing names, nationalities and facial images, as mentioned above, which shows that not only the purpose of the database is broadened, but also the type of data it stores. There are several reasons why biometric systems use fingerprints: they are easy to collect and not easily modified by illness

---

with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), (COM(2016)0272 – C(- 0179/2016 – 2016/0132(COD)) Brussels, 12 June 2017.

[74] *Ibid*., point 22 a.

[75] *Ibid*., Articles 9 and 14.

[76] *Ibid*., Article 11.

or ageing, for example.[77] Public security concerns and counter terrorism measures are reasons that justify the resource and willingness to expand the use of biometric data as it contributes to make "asylum proceedings easier and faster".[78]

Several concerns have been raised in the literature regarding the inclusion of biometric data in SIS II, which are also shared when one thinks of the application of VIS and EURODAC.[79] The EDPS pointed out in his Opinion on the draft SIS II legislation: "(…) the tendency to use biometric data in EU wide information systems (VIS, EURODAC, Information System on driving licences, etc.) is growing steadfastly, but is not accompanied by a careful consideration of risks involved and required safeguards".[80]

The lack of consideration of the risks involved, as the EDPS put it, intrinsically relates to the risk of lack of accuracy that may result from a biometric search. Problems with accuracy are probably the greatest weakness of the use of biometrics.[81] Biometrics is a sophisticated means of identification of people, and the use of biometric data is a very valuable tool for identity control, although it can also negatively affect their legal position if there is any failure in the procedure. The EDPS argued that in case of failure to register the fingerprints of an asylum seeker due to, for example, an incorrect identification this should not lead to a rejection or refusal of his or her application.[82] In relation to biometrical data, the CJEU stated in 2013 in the *Schwarz* decision that although the taking and storing of

---

[77] Lehte Roots, "The new EURODAC regulation: Fingerprints as a source of informal discrimination", *Baltic Journal of European Studies Tallinn University of Technology* 5, no. 2 (2015): 111.

[78] *Ibid*., 112.

[79] *Ibid*., 53. Tzanou, "The added value of data protection as a fundamental right in the EU legal order in the context of law enforcement", 199-203; Peers, Guild and Tomkin, *EU Immigration and Asylum Law*, 114, Besters and Brom, "Greedy information technology: The digitalization of the European migration policy", 458-459. In relation to VIS and the use of biometrics: Baldaccini, "Counter-terrorism and the EU strategy for border security: Framing suspects with biometric documents and databases", 38 and 49.

[80] Opinion of the European Data Protection Supervisor on the draft SIS II legislation, OJ 91/38, 2006, point 4.1, and Memorandum by the Meijers Committee, House of Lords European Union Commitee, Schengen Information System II (SIS II), 10 of July 2006, 4, (http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/49/6101107.htm).

[81] Yue Liu, "Scenario study of biometric systems at borders", *Computer Law & Security Review* 36 (2011): 42.

[82] Opinion of the European Data Protection Supervisor on the amended 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. [.../...] [...] (Recast version), 2012, 17.

fingerprints by the nationals authorities "constitutes a threat to the rights to respect for private life and the protection of personal data", it must nevertheless be assessed if that measure is justified.[83] The unique nature of biometric data, which allows a more precise identification of individuals, was already stressed above when discussing the *S. & Marper* case – a point also made by the CJEU – and, for that reason, requires additional concerns as regards the necessity and proportionality of its usage.[84]

Other critiques are also commonly put forward in relation to the use of biometrical data. Firstly, there is the risk that criminal organisations may have easier access to biometrical data and misuse or manipulate it, as well as of an increase in identity theft.[85] Secondly, one may also think of the possibility of transforming EU databases into systems used by law enforcement authorities as profiling tools. Thirdly, the risk of biometrics misuse rises when the data is stored in a centralised database, such as EURODAC, due to the fact that there is a bigger risk of unlawful access to the information.[86] Lastly, it has been pointed out that the recourse to technology may lead to the "dehumanization of individuals via the instrumentalization of the human body", contributing to the practice of asylum-seekers deliberately mutilating their fingerprints, and to providing the States with personal data that can be accessed in different instances.[87]

The 2016 recast EURODAC Regulation proposal introduces the requirement to store facial images in addition to fingerprints to overcome certain difficulties encountered by Member States with the fingerprinting of applicants and to speed up the process, even though the comparison of facial images without fingerprints should be a last resource measure for Member States.[88] This inclusion on the EURODAC Regulation proposal reflects the need to establish a division between solutions that aim to address administrative issues such as the failure of fingerprinting and the necessity of

---

[83] Judgment of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, EU:C:2013:670, paragraph 23.

[84] *Ibid*., paragraph 27.

[85] Steve Peers, Elspeth Guild and Jonathan Tomkin, *EU Immigration and Asylum Law* (Brill, 2012), 116.

[86] Roots, "The new EURODAC regulation: Fingerprints as a source of informal discrimination", 126.

[87] Valsamis Mitsilegas, "Immigration control in an era of globalization: Deflecting foreigners, weakening citizens, strengthening the State", *Indiana Journal of Global Legal Studies* 19, (2012): 37, and for more in the same topic see Huub Dijstelbloem, "Europe's new technological gatekeeper. Debating the deployment of technology in migration policy", *Amsterdam Law Forum* 1 (2009), http://amsterdamlawforum.org/article/view/90/154.

[88] Recital 10 and Articles 2 (1) and 16 (1) of the 2016 recast EURODAC Regulation proposal.

collecting more biometrics identifiers, in this case by EURODAC, at the risk of disrespecting Articles 7 and 8 of the Charter of Fundamental Rights. Against this scenario, Aas' view is even more relevant: "the body becomes, in a sense, a passport or a password and an unambiguous token of truth",[89] immigration control databases coincide with the concept of borders as these are in the end tools for the categorisation of migrants. In the case of asylum seekers, "the traveller embodies the border"[90] and EURODAC is foremost an example of the establishment of a personalised (and digital) border.

4. *The impact of the development of EURODAC in EU Migration Law*

After analysing in specific the most recent amendments to the EU asylum fingerprinting system *vis-à-vis* the principle of purpose limitation, and the proportionality and necessity of the expansion of the scope of the EURODAC biometric database, two main aspects within EU migration can be highlighted: the potential criminalisation and stigmatisation of asylum seekers and irregular migrants and the securitisation of EU migration law.

Firstly, the criminalisation of irregular migrants is not an isolated trend in the domestic immigration law of any particular State. In fact, this phenomenon is a "widespread trend all over the world".[91] Criminal law that prosecutes immigration offences is a key aspect of the criminalisation of migration.[92] Throughout this study it has been argued that the fact that asylum seekers and irregular migrants whose biometric data is collected by EURODAC and accessed by national and European law enforcement authorities puts this group of travelers under greater suspicion than others whose data will not be requested to compare for criminal purposes. Yet, this practice is neither an express or substantive criminalising measure, nor is it illegal or discriminatory *per se*. Law enforcement authorities' access to the EURODAC system serves legitimate goals such as the prevention, detection or investigation of terrorist offences or other serious criminal offences; yet, it is important to understand that there are implications

[89] Katja Franko Aas, "'The body does not lie': Identity, risk and trust in technoculture", *Crime, Media, Culture* 2 (2006): 145.

[90] Ferraris, "Economic migrants and asylum seekers in ten fingers: Some reflections on Eurodac and border control", 5.

[91] Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice* (Springer, 2011), 280.

[92] Valsamis Mitsilegas, *The Criminalisation of Migration in Europe* (Springer, 2015), 77.

and a "high risk" of treating asylum seekers as criminals if control over the access to this data is not exerted in a rigorous way.[93]

Another aspect that contributes to the stigmatisation of asylum seekers and irregular migrants, and which is a consequence of the *modus operandi* of the immigration databases, in particular of EURODAC, is a depersonalisation of the individuals whose data is stored. With regard to the depersonalisation of migrants, it can be said that this has a generalising effect (or profiling) of categorising people in a manner not regulated by law. The depersonalisation of mobile individuals is related to the creation of migrant profiles such as "the suspected" or "mala fide", the "trusted" or "bona fide traveller",[94] or the "crimmigrant".[95] This trend has a strong stigmatising effect on migrants categorising them *ab initio* and socially excluding individuals who are not a perfect fit for these profiles. As such, the personal element loses its relevance: "the migration machine by its nature tends to dehumanize the people it needs to process".[96]

Secondly, and equally important, is the recent development of the framework of immigration databases which has led to the enhancement of migration governance securitisation. With regard to the issue of the way EU immigration databases shape, for example, the illegality of one's stay, it is safe to argue that the prevalence of surveillance in its framework is enough to say that, once more, the status of illegality has not developed completely independently from security concerns.

This issue is particularly important when one examines EURODAC's shift for a broader and more securitarian purpose which allows access to biometric data for security purposes, but this is also true in what regards EUROSUR. The EUROSUR Regulation was approved by the European Parliament in October 2013 and applicable from December 2013 in certain Member States.[97] EUROSUR's purpose is established in Article 1 of the

---

[93] Roots, "The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination", 125.

[94] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration, 2011, point 34.

[95] Katja Franko Aas, "Crimmigrant' bodies and bona fide travelers: Surveillance, citizenship and global governance", *Theoretical Criminology* 15, no. 3 (2011), 336 and 338.

[96] Huub Dijstelbloem and Albert Meijer, "Reclaiming control over Europe's technological borders", in Huub Dijstelbloem and Albert Meijer, *Migration and the New Technological Borders of Europe*. (Palgrave MacMillan, 2011), 184.

[97] In Bulgaria, Estonia, Greece, Spain, France, Croatia, Italy, Cyprus, Latvia, Lithuania, Hungary, Malta, Poland, Portugal, Romania, Slovenia, Slovakia and Finland. In the remaining Member States, EUROSUR was applicable since 1 December 2014.

Regulation as "detecting, preventing and combating illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants".[98] EUROSUR does pursue the humanitarian purpose of protecting and saving migrants' lives and it stresses the need to comply with fundamental rights and to prioritise vulnerable groups; yet, how this could be achieved is not described in the Regulation.

Contrariwise, the EUROSUR Regulation places a stronger emphasis on the issue of surveillance. In fact, the Commission's proposal of 2011 included a reference to migrant profiling establishing that the national situational picture "shall contain migrant profiles, routes, information on the impact levels attributed to the external land and sea border sections and facilitation analysis".[99] This formulation was later excluded from the final version of the EUROSUR Regulation, Article 5(3)(b) of which ensures "the timely exchange of information with search and rescue, law enforcement, asylum and immigration authorities at national level". Mitsilegas argues that merging "the logic of risk prevention with the logic of border security" in relation to these new models of surveillance may have implications for the protection of fundamental rights, in particular with regard to asylum seekers and to "the relationship between the individual and the state".[100]

Thus, it can be argued that it is not only those databases already established, such as EURODAC, that view information technology systems as identification tools with a particular focus on the removal of migrants, on impeding their entrance or law enforcement purposes, but also the new generation of immigration databases (for example EUROSUR), which follow the same archetype despite their humanitarian concerns.

5. Conclusion

What can be concluded from the most recent EU strategy for border control asylum information systems? The fact that one can identify the trends previously addressed as factors of the conflation of asylum seeking and criminality in recent proposals and amendments of the EURODAC

---

[98] European Parliament and Council Regulation of the (EU) No. 1052/2013 establishing the European Border Surveillance System (Eurosur), [2013], OJ L295/1.

[99] Article 6 c) of the European Commission proposal for a Regulation establishing the European Border Surveillance System (COM (2011) 0873) and Meijers Committee for a Regulation establishing the European Border Surveillance (COM (2011) 0873), CM1215, 12 September 2012, 1 and 4.

[100] Valsamis Mitsilegas, "The borders paradox: The surveillance of movement in a Union without internal frontiers", *A Right to Inclusion and Exclusion? Normative Faultlines of the EU's Area of Freedom, Security and Justice*, Hans Lindahl (eds.), (Hart, 2009), 61.

Regulation reflects a common premise of the present study: the potential digital criminalisation and stigmatisation of asylum seekers and illegally staying migrants. This scenario is illustrative of the so-called *crimmigration* phenomenon.[101] There is a clear trend identified by the literature of criminalising immigration offenses at a national level in the EU,[102] and this study aimed to show how, at the level of the management of supranational structures of surveillance in the area of justice and home affairs, especially with regard to EURODAC, some practices can potentially lead to the same (criminalising) result at the EU level.

The fact that the EU system of surveillance puts some categories of mobile people under greater surveillance than others is clear for all to see. The story of mass surveillance and digital borders continues to be written under the premise that irregularity and criminality can be put under the same degree of suspicion, as we have seen, for instance, with regard to asylum seekers and irregular migrants, whose fingerprints are collected by the EURODAC system, to which national law enforcement authorities and Europol are gradually gaining broader and simpler access. This is so regardless of the legitimate goals that the Commission aims to achieve, such as facilitating the application of the Dublin system, in particular after the 2015 mass influx of asylum seekers in the EU.

At the centre of this study is the idea that EU instruments in charge of regulating EU immigration databases influence the legal regime and the categorisation of asylum seekers and irregular migrants. In relation to the changes and the recent proposal for amendment of the EURODAC Regulation, this argument was evidenced by three main trends common to these databases: the erosion of the principle of purpose limitation, the widening of access to data by law enforcement authorities, and the impact of the digitalisation of borders through biometrics.

Since 2017, trilogues are ongoing on the amendment of EURODAC proposed in 2016 by the EU Commission, guaranteeing not only that the system respects the fundamental rights of migrants, but also the principles of data protection are a priority of the co-legislators. Whereas a provisional agreement between the Parliament and the Council was reached in June 2018 regarding the storage of fingerprints, facial images and alphanumeric data of asylum seekers and irregular migrants, the age for

[101] *Ibid*., 379.

[102] Perrine Dumas, *L'Accès des Ressortissants des Pays Tiers au Territoire des États Membres de l'Union Européenne* (Bruylant, 2013), 310.

obtaining fingerprints lowered to 6 years old, and a more efficient access to the database by Europol, it is crucial to guarantee a reinforced supervision of the treatment of this data and of the way it is collected at a national level. Taking into consideration the scope of other changes put forward by the 2016 EURODAC proposal, for example, giving the authorities of third countries partial access under certain conditions and the use of detention and coercion as last resort to ensure the fingerprinting of migrants, the EU has the duty to reinforce safeguards to guarantee the respect for the fundamental rights of the people involved in these procedures in the reception facilities, in particular at the national level.[103]

Trying to address the reform of the Dublin system through continuously expanding the purpose and access to what should be an administrative tool such as EURODAC will only result in a temporary quick fix to an asylum system that needs a structural reform. The trends that result from EURODAC's framework impact on EU Migration Law, namely the stigmatisation of asylum seekers and irregular migrants and the securitisation of EU migration can be found also in the EU's new surveillance initiatives, such as the EUROSUR (the European Border Surveillance System). If these are continuously reproduced, the potential criminalisation and stigmatization will continue to represent one of the biggest challenges of the EU policy Agenda. The risk of amending the European Common Asylum System based on these trends is a dangerous one and a high price to pay in terms of the protection of the fundamental rights of asylum seekers and irregular migrants.

Bibliography

Abelson, Hal, Ken Ledeen and Harry R. Lewis. *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion*. Boston: Addison-Wesley Professional, 2008.

Amoore, Louise. "Biometric borders: Governing mobilities in the war on terror". *Political Geography* 25 (2006).

Baldaccini, Anneliese. "Counter-terrorism and the EU strategy for border security: Framing suspects with biometric documents and databases". *European Journal of Migration and Law* 10 (2008).

Barbou des Places, Ségolène. "Evolution of asylum legislation in the EU: Insights from regulatory competition theory". *RSCAS Working Paper* 16 (2003).

[103] Both the European Parliament and the EU's Agency for Fundamental Rights have questioned the necessity and proportionality of using physical or psychological force to obtain fingerprints.

Besters, Michiel and Frans WA Brom. "Greedy information technology: The digitalization of the European migration policy". *European Journal of Migration and Law* 12 (2010).

Betts, Alexander and Paul Collier. *Refuge – Transforming a Broken Refugee System*. London: Penguin Books, 2017.

Boehm, Franziska. *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*. Berlin, Heidelberg: Springer, 2011.

Broeders, Dennis. "A European 'border' surveillance system under construction. In *Migration and the New Technological Borders of Europe. Migration, Minorities and Citizenship*, edited by Huub Dijstelbloem and Albert Meijer. London: Palgrave Macmillan, 2011.

Broeders, Dennis. *Breaking Down Anonymity: Digital Surveillance on Irregular Migrants in Germany and the Netherlands*. Amsterdam: Amsterdam University Press, 2009.

Brouwer, Evelien Renate. *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, vol 15. Leiden: Brill, 2008.

Brouwer, Evelien Renate. "Eurodac: Its limitations and temptations". *European Journal of Migration and Law* 4 (2002).

Brouwer, Evelien Renate. "Legality and data protection law: The forgotten purpose of purpose limitation". In *The Eclipse of the Legality Principle in the European Uni*on, edited by Leonard F. M. Besselink, Frans Pennings and Sacha Prechal. Alphen aan den Rijn: *Kluwer Law* International, 2011.

Dijstelbloem, Huub. "Europe's new technological gatekeeper. Debating the deployment of technology in migration policy", *Amsterdam Law Forum* 1 (2009) (http://amsterdamlawforum.org/article/view/90/154).

Dijstelbloem, Huub and Albert Meijer. "Reclaiming control over Europe's technological borders". In *Migration and the New Technological Borders of Europe*, edited by Huub Dijstelbloem and Albert Meijer. London: Palgrave MacMillan, 2011.

Dumas, Perrine. *L'Accès des Ressortissants des Pays Tiers au Territoire des États Membres de l'Union Européenne*. Brussels: Bruylant, 2013.

Ferraris, Valeria. "Economic migrants and asylum seekers in ten fingers: Some reflections on Eurodac and border control", 2017, https://www.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2017/05/economic-migrants.

Franko Aas, Katja. "Crimmigrant bodies and bona fide travelers: Surveillance, citizenship and global governance". *Theoretical Criminology*, 15(3) (2011).

Franko Aas, Katja. "'The body does not lie': Identity, risk and trust in technoculture", *Crime, Media, Culture* 2 (2006): 143.

Leun, Joanne van der, and Maartje van der Woude. "A reflection on crimmigration in the Netherlands". In *Social Control and Justice – Crimmigration in the Age of Fear*, edited by Maria João Guia, Maartje van der Woude and Joanne van der Leun. The Hague: Eleven International Publishing, 2013.

Liu, Yue. "Scenario study of biometric systems at borders". *Computer Law & Security Review* 27 (2011).

Mitsilegas, Valsamis. "Immigration control in an era of globalization: Deflecting foreigners, weakening citizens, strengthening the State". *Indiana Journal of Global Legal Studies* 19 (2012).

Mitsilegas, Valsamis. "The borders paradox: The surveillance of movement in a Union without internal frontiers". In *A Right to Inclusion and Exclusion? Normative Faultlines of the EU's Area of Freedom, Security and Justice*, edited by Hans Lindahl. Oxford: Hart Publishing, 2009.

Mitsilegas, Valsamis. *The Criminalisation of Migration in Europe*. Springer, 2015.

Peers, Steve, Elspeth Guild and Jonathan Tomkin. *EU Immigration and Asylum Law.* Brill, 2012.

Rijpma, Jorrit. "Building borders: The regulatory framework for the management of the external borders of the European Union". PhD dissertation. Florence: European University Institute, 2009.

Roots, Lehte. "The new EURODAC regulation: Fingerprints as a source of Informal discrimination". *Baltic Journal of European Studies Tallinn University of Technology* 5, no. 2 (2015).

Stumpf, Juliet. "The crimmigration crisis: Immigrants, crime, & sovereign power". *American University Law Review* 56 (2006).

Tzanou, Maria. "The added value of data protection as a fundamental right in the EU legal order in the context of law enforcement". PhD dissertation. Florence: European University Institute, 2012.