

## OF BIOMETRIC DOCUMENTS, DATABASES AND FREE MOVEMENT OF PERSONS IN THE EU\*

**Alessandra Lang, PhD, Associate Professor**

University of Milan, Department of International,  
Legal, Historical and Political Studies  
Via Conservatorio 7, 20 122 Milan, Italy  
alessandra.lang@unimi.it

### **ABSTRACT**

*Free movement of persons is a right recognised by the Treaty on the Functioning of the European Union (TFEU) for EU nationals (and their family members, irrespective of their nationality), and is one of the rights related to EU citizenship. Being an EU national is the qualifying element to benefit from the free movement regime, which is more favourable than the immigration regime otherwise applicable to foreigners. In order to prove one's nationality, identity cards and passports play a central role. The issuance of these documents is regulated by national law. Over the last 20 years, EU law has intervened in this area with the aim of strengthening the document security. In 2004, the EU institutions passed a regulation on biometric passports and in 2019 a regulation on biometric identity cards. From now on, the facial image and fingerprints data of the holder are kept in the storage medium in these documents. The reasons for the introduction of biometric data lie in preventing the falsification of the document and the fraudulent use of authentic documents. On the one hand, the techniques used to preserve and protect the data make these documents more difficult to forge. On the other hand, the presence of biometric data creates a reliable link between the holder and the person who owns the document, thus making it easier to identify the person, and more difficult to use the document fraudulently by those who are not the real holder.*

*Meanwhile, the EU is promoting the interoperability of the many databases established over-time. Interoperability connects different databases and makes the data stored in them searchable and accessible to a wider range of authorities and for other purposes than those for which they are collected. Biometric data, such as facial images and fingerprints are stored in many databases.*

*The paper will sketch out the interference of the two issues (biometric documents and databases) in relation to the free movement of persons, in order 1) to map the instances in which*

---

\* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

*controls on biometric documents of EU nationals or family members lead to search in the databases, and 2) to assess the impact that the very existence of biometric documents and databases can have on the fundamental rights of individuals.*

**Keywords:** *biometrical documents, databases, EU citizenship, EU nationals, fingerprints, free movement of persons*

## 1. INTRODUCTION

Free movement of persons allows Union citizens and their family members to travel between Member States and to move to a different Member State from their country of origin, thanks to their nationality. Identity documents are important because they are the primary way of proving the holder's nationality. In recent years, the European Union has stipulated that any identity documents (passports and identity cards) issued by Member States must contain biometric data. This article seeks to explore the basis for this legislation and to assess whether it provides reliable guarantees that the biometric data collected for inclusion in identity documents is not stored in databases.

## 2. IMPORTANCE OF IDENTITY DOCUMENTS FOR FREE MOVEMENT OF PERSONS

Identity documents have an important function in the free movement of persons because they are the primary way of proving the identity and citizenship of their holders. Citizenship, in turn, is the determining factor for applying the EU laws on citizenship rights, first and foremost among which is the right to free movement of persons. This right is now enshrined in Article 21 TFEU and Article 45 CFREU, and is regulated by Directive 2004/38.<sup>1</sup> Free movement means that Union citizens have the right to leave their home State and enter and reside in another Member State. Correlatively, Member States are obliged to grant Union citizens rights of exit, entry and residence under the conditions laid down in EU law. This right is neither unconditional nor unlimited. EU law itself provides that Union citizens must meet the conditions required to exercise the rights attached to free movement. These conditions are that individuals claiming free movement rights must be Union citizens, proven by an identity document, and must, for periods of residence of longer than three months, prove that they fall into one of the

---

<sup>1</sup> Directive 2004/38/EC of the European Parliament and of the Council on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC [2004] OJ L 158/77. Guild, E.; Peers, S.; Tomkin, J. (eds.), *The EU citizenship directive: a commentary*, Oxford University Press, Oxford, 2<sup>nd</sup> ed., 2019.

following categories: workers or self-employed persons, students with sufficient resources and sickness insurance, persons who are economically self-sufficient (because they have sufficient resources and sickness insurance) or family members of a Union citizen who falls into one of the three categories mentioned above. On the other hand, free movement rights may be restricted by States on grounds of public policy, public security and public health, subject to the safeguards provided for in EU law.

Directive 2004/38 sets out the administrative formalities that the host State may require Union citizens to fulfil. Specifically, a Union citizen who is intending to reside for longer than three months may be required to register with the relevant authorities. In this way, the host State can verify that the Union citizen meets the substantive requirements laid down in EU law and can release a residence certificate.

As far as treatment is concerned, the Directive provides that Union citizens are entitled to equal treatment with host State nationals, albeit with certain restrictions (art. 24). After five years of legal and continuous residence, Union citizens acquire the right of permanent residence (Art. 16), which sees an improvement in their legal status. For example, the right of permanent residence is no longer conditional on meeting the criteria for periods of residence of more than three months (that is, being a worker, a student or economically self-sufficient), equal treatment applies without restrictions of any kind and Union citizens qualify for enhanced protection against expulsion.

How the host State treats non-citizens depends primarily on citizenship. Applying the rules on free movement or immigration depends on the person's citizenship above and beyond any personal characteristics. It comes as no surprise, therefore, that some people seeking to take advantage of the more favourable free movement rules are prepared to engage in illegal behaviours in order to obtain a document certifying that they hold Union citizenship, such as using counterfeit documents or fraudulently using genuine documents. The Member States are very concerned about this risk, and this may explain why there is an increasing focus on biometric documents, the subject-matter of this article.

As far as identity documents are concerned, Directive 2004/38 states that possession of a passport or identity card proving the holder's nationality is a necessary and sufficient condition for exercising the right to leave the country of origin or residence (Article 4(1)),<sup>2</sup> to enter another Member State (Article 5(1))<sup>3</sup> and to

---

<sup>2</sup> The article goes on to say that States cannot impose any exit visa or equivalent formality.

<sup>3</sup> This article also prohibits States from imposing entry visas or equivalent formalities. An identity card is therefore a travel document, in the same way as a passport, and not just an identity document.

reside in another Member State for up to three months (Article 6(1)) and is a necessary but not sufficient condition for a period of residence of more than three months (Article 8(3)). Member States are obliged to issue passports or identity cards to their citizens.<sup>4</sup> Issuing documents is a matter of national competence, but States must do this in a way that does not undermine the rights that Union citizens derive from EU law. Since the prerequisite for exercising the right is possession of a document that only national authorities can issue, the Court of Justice considers that a State cannot impose conditions which, if not satisfied, would entitle it to refuse to issue an identity document to its citizens.<sup>5</sup>

The State which issued the identity document is also obliged to allow the holder who has been expelled from another Member State to re-enter its territory, without being able to raise any objections over the validity or authenticity of the document (Article 27(4)).

The Court of Justice has clarified the *ratio* and scope of the requirement to hold a passport or identity card. It has stated that free movement is a right of Union citizens and that States may demand proof of citizenship. Possession of an identity document is an administrative formality that facilitates free movement by making it easier to identify the beneficiaries.<sup>6</sup> Lack of a valid passport or identity card may be sanctioned as an administrative offence, but the State cannot claim that the person is not entitled to free movement. Since the right to free movement is a consequence of citizenship, and passports and identity cards are merely means of evidence, the Court concludes that the State must give the person every opportunity to prove their identity in some other way.<sup>7</sup> Accordingly, the State should also

---

Passports are travel documents accepted by States as a matter of comity (see Hagedorn, C., *Passport*, Max Planck Encyclopedia of Public International Law, 2008, para. 7), whereas identity cards fulfil this function between States that accept them, usually in accordance with an international agreement but also (as in this case) under EU law.

<sup>4</sup> Similar provisions had previously been included in Article 2(2) of Directive 68/360 on the free movement of workers and Article 2(2) of Directive 73/148 on the right of establishment and the free movement of services, whereas the directives issued in the 1990s extending free movement to students (Directive 93/96), pensioners (Directive 90/365) and economically self-sufficient persons (Directive 90/364) contained no provisions to that effect.

<sup>5</sup> See, in particular, Case C-490/20 *Stolichna obshtina, rayon 'Pancharevo'* [2021] ECLI:EU:C:2021:1008, par. 45.

<sup>6</sup> Case C-35/20 *A* [2021] ECLI:EU:C:2021:813, par. 53.

<sup>7</sup> Case C-215/03 *Oulane* [2005] ECLI:EU:C:2005:95 par. 23, which cites as precedent case C-459/99 *MRAX* [2002] ECLI:EU:C:2002:461, par. 62, a statement later codified in Article 5(4) of Directive 2004/38. So, while the directive sets out this principle in cases where a Union citizen does not have any documents at the time of entry, under the *Oulane* case law, a similar principle applies when the person is already in the country and must prove their right of residence.

accept documents that are not valid for leaving the country<sup>8</sup> or other documents that are means of evidence of identity under national law (such as driving licences in some States).

EU law requires States to recognise the validity of travel and identity documents issued by other Member States, unless there are justified reasons to believe that a certain document has been falsified.<sup>9</sup> A falsified document may constitute a case of fraud which, under Article 35 of Directive 2004/38, justifies the refusal of free movement rights.<sup>10</sup>

Family members of Union citizens, regardless of their nationality, also benefit from these special legal rules. They enjoy freedom of movement in order to enable their relative, a Union citizen, to enjoy family unity even if that person moves to another Member State. The right to family reunification (within its broad meaning of the right to accompany a relative or to be reunited with a relative) has, since the very beginning of free movement, been portrayed first and foremost as a right for migrant workers and then as a right for Union citizens. It follows that family members do not enjoy free movement rights independently but only if they are travelling and residing with a Union citizen or they move to reunify with a Union citizen. In these cases, their legal status is equivalent to that of a Union citizen and they are exempt from the less favourable immigration rules. The discriminating factor between applying free movement of persons and immigration law is not the person's nationality but rather their family ties. For this reason, States want, on the one hand, to exercise a certain control over family members and, on the other hand, to counter behaviour such as sham marriages or adoptions as a means of pre-establishing family ties.<sup>11</sup> Directive 2004/38 contains a number of specific provisions to reassure the concerns of the Member States: firstly, the only

---

<sup>8</sup> Case C-376/89 *Giagounidis* [1991] ECLI:EU:C:1991:99, par. 16.

<sup>9</sup> Case C-202/13 *McCarthy* [2014] ECLI:EU:C:2014:2459, par. 58. The principle, expressed in relation to the residence cards of family members (see below), can also be extended to identity documents.

<sup>10</sup> "In the context of the Directive, fraud is likely to be limited to forgery of documents or false representation of a material fact concerning the conditions attached to the right of residence": Communication from the Commission to the European Parliament and the Council on guidance for better transposition and application of Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States, COM/2009/313 final.

<sup>11</sup> Pursuant to Article 35 of the Directive, Member States can deny or revoke the right of residence in these cases. See Commission Staff Working Document, Handbook on addressing the issue of alleged marriages of convenience between EU citizens and non-EU nationals in the context of EU law on free movement of EU citizens, SWD/2014/284.

travel and identity document stipulated by the directive is a passport and not a passport as well as an identity card;<sup>12</sup> secondly, entry into the State may be subject to possession of a visa, regardless of the family member's place of residence, in cases where EU or national law requires this for entry from a third country (Article 5(2)).<sup>13</sup> There is, however, an exception, which benefits family members who hold a residence card, in other words family members who are resident with their spouse in a Member State of the European Union, having exercised their right to free movement.<sup>14</sup> Hence the importance of a residence card and the fears of falsification or fraudulent use which will be discussed further below. Thirdly, exercise of the right of residence for family members is subject to the performance of more onerous formalities than those existing for Union citizens. These include applying for and being issued with a residence card (and not just registering with the national authorities), as a means of further checking someone's identity and the potential danger that person poses, albeit that a residence card does not give rise to a right of residence but is merely of a declaratory nature.<sup>15</sup>

### 3. BIOMETRIC DOCUMENTS

Despite the importance of identity documents for free movement of persons, the rules governing identity documents have remained within the competence of the Member States. That is not to say that the Union has had no involvement in this area. In the 1980s, a uniform passport, largely symbolic in value, was established in order to create an outward and common mark of citizenship.<sup>16</sup> In the aftermath of the 9/11 attacks, the Western world felt the need for increased security, resulting in more extensive checks on those entering the country. The terrorist threat came

<sup>12</sup> For exit (Article 4(1)), entry (Article 5(1)), residence of less than three months (Article 6(2)) and residence of more than three months (Article 10). The directive is not therefore the basis for recognition of identity cards as a travel document into and within the Union.

<sup>13</sup> These are the cases covered by Regulation 2018/1806, which lists the States whose nationals must be in possession of visas when crossing the external borders including for short-stay visits. Ireland is the only State not bound by the Regulation, as it does not participate in the Schengen acquis. States are obliged to grant a visa to the family member, who must only apply for a short-stay visa, even if the intention is to stay for longer: Case C-157/03 *Commission v Spain* [2005] ECLI:EU:C:2005:225, par. 38.

<sup>14</sup> Article 5(1) mentions only a residence card issued for a period of residence of more than three months, and not a permanent residence card, which is issued to the family member after five years of legal and continuous residence in accordance with Article 20. However, in Case C-754/18 *Ryanair Designated Activity Company* [2020] ECLI:EU:C:2020:478, par. 38, the Court stated that a permanent residence card also exempts a person from possessing a visa, rejecting the formalistic arguments put forward by the State concerned.

<sup>15</sup> Case C-246/17 *Diallo* [2018] ECLI:EU:C:2018:499, par. 48.

<sup>16</sup> Resolution of the Representatives of the Governments of the Member States of the European Communities, meeting within the Council 1981 [1981] OJ C 241/1. See Herting Randall, M.; Hänni, D.; *European Passport*, Max Planck Encyclopedia of Public International Law, 2019.

from outside and had to be stopped from entering. Leading the way, of course, was the United States, which introduced biometric passports and demanded that everyone entering the country must have one.<sup>17</sup> The European Union followed in its footsteps, so as to enable EU citizens to enter the United States. The inclusion of biometric data (facial image and fingerprints),<sup>18</sup> firstly in travel documents and later in identity documents, is justified by the need to make documents more secure (less falsifiable) and identity theft (preventing the use of another person's document) more difficult.<sup>19</sup> Biometric data is interesting because it can be taken from practically anyone, the technology for collecting, storing and reading it is well developed and biometric data is characterised by a certain (albeit not absolute) stability over time, which means that it can be compared with outcomes that are considered broadly reliable.

The biometric documents governed by EU law which will be considered here are passports, identity cards and residence cards of family members of Union citizens. The first two are both travel documents and identity documents.<sup>20</sup> Residence cards are neither one nor the other but when combined with a passport, their holder is treated as a Union citizen when crossing an external border, either coming in or going out (see below) and is exempt from the need to obtain a visa to cross the internal borders.

### 3.1. Biometric passports

Regulation 2252/2004,<sup>21</sup> amended by Regulation 444/2009<sup>22</sup> (containing highly appropriate amendments, as discussed in section 5.1.1), covers biometric pass-

<sup>17</sup> Torpey, J., *The invention of the passport: surveillance, citizenship, and the state*, Cambridge University Press, Cambridge, 2018, pp. 195 - 206.

<sup>18</sup> For a discussion on the technical and legal meaning of the notion, as well as on the different use of terms between biometric experts and data protection lawyers, see Jasserand, C., *Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data*, European Data Protection Law Review, Vol. 2, No. 3, 2016, pp. 297-311.

<sup>19</sup> However, it is debatable that biometric data makes documents more difficult to falsify: see Baechler, S., *Document Fraud: Will Your Identity Be Secure in the Twenty-first Century?*, European Journal on Criminal Police and Research, Vol. 26, 2020, pp. 379 – 394.

<sup>20</sup> At the same time, the EU is working on digital identity to access goods and services: Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73. Since this subject is unrelated to travel or identity documents, it will not be discussed in this paper.

<sup>21</sup> Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L 385/1.

<sup>22</sup> Regulation (EC) No 444/2009 of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and

ports. The Regulation does not establish a common model (which already exists) but merely provides that passports issued by Member States must contain a facial image and two fingerprints (Article 1), collected by authorised staff (Article 1a) and stored on a highly secure storage medium in the passport (Article 1). Technical characteristics are regulated through the Commission's implementing acts (Article 5). The Regulation also provides that children under the age of 12 years and persons for whom fingerprinting is impossible are exempt from the requirement to give fingerprints (Article (1)(2a)). The passport contains only the machine-readable information provided for in the Regulation or under national legislation (Article 4(2)). Access to biometric data is only permitted to verify the authenticity of the document and the identity of the holder (Article 4(3)). The Regulation does not stipulate which authorities may access this data but states that this is determined by the Member States (recital 4).

The Regulation does not establish the conditions for issuing passports or the data that must or may be contained in such documents. This is left to the discretion of the Member States, although reference can be made to ICAO Document 9303, which aims to standardise the information contained in travel documents in order to make them machine-readable.<sup>23</sup> According to the Court of Justice, the Regulation requires that the machine-readable biographical data page of passports issued by Member States must comply with the specifications for machine-readable passports laid down in Part 1 of ICAO Document 9303 and must satisfy all of the compulsory specifications provided for therein.<sup>24</sup> Thanks to the reference made by the Regulation, ICAO Document 9303 thus becomes binding on the Member States.<sup>25</sup>

---

travel documents issued by Member States [2009] OJ L 142/1.

<sup>23</sup> The International Civil Aviation Organization (ICAO) is responsible for ensuring the orderly and safe development of international civil aviation, in particular through the adoption of international standards and recommendations, which may also include immigration formalities (Article 37(i), Convention on International Civil Aviation, Chicago, 7-12-1944). Document 9303 is one such recommendation. Pursuant to Article 23 of the Chicago Convention, States undertake to enact, where they deem this appropriate, immigration regulations that are consistent with ICAO recommendations. If States consider that they can comply with ICAO recommendations, they must, under Article 38, notify the ICAO of the differences between their own regulations and the ICAO recommendations. Abeyratne, R.I.R., *The Development of the Machine Readable Passport and Visa and the Legal Rights of the Data Subject*, *Annals of Air and Space Law*, Vol. 17, Part 2, 1992, at 1, points out that machine-readable documents have been envisaged as a tool to facilitate international air transport and tourism; hence the role played by ICAO.

<sup>24</sup> Case C-101/13 *U* [2014] ECLI:EU:C:2014:2249, paras. 23-24.

<sup>25</sup> Hornung, G., *Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues*, *European Public Law*, Vol. 11, 2005, p. 504.

### 3.2. Biometric identity cards

In 2019, the EU established a uniform format for identity cards<sup>26</sup> on which the holder's biometric data is stored. Without affecting the obligation to hold an identity card (applicable in all Member States except Denmark), the Regulation requires States to use the harmonised format when issuing documents and to progressively withdraw documents with a different format.<sup>27</sup> The format to be used is not brand new but is the same as that previously provided for in Regulation 1030/2002,<sup>28</sup> to which must be added "the two-letter country code of the Member State issuing the card, printed in negative in a blue rectangle and encircled by 12 yellow stars" (Article 3(4)). It should be noted that Regulation 1030/2002 concerns residence permits, which are essential for managing immigration policy but whose function is not comparable to an identity card and they are not normally used on their own but always accompanied by a passport.

Regulation 2019/1157 is very similar to Regulation 2252/2004. The inclusion of biometric data is justified for the same purposes, namely to make it more difficult to falsify documents and to use genuine documents fraudulently (recital 18) and access to data is only allowed for the same purposes (Article 11(3)).

Just like the Regulation on passports, this Regulation provides that identity cards issued by Member States must include a highly secure storage medium containing a facial image and two fingerprints (Article 3(5)) collected by authorised staff (Article 10(1)), according to procedures that respect fundamental rights (Article 10(2)). The Regulation also provides for exemptions from the requirement to give fingerprints (for children under the age of 6 years, a limit which States may raise to 12 years, and for persons in respect of whom fingerprinting is impossible: Article 3(7)). But unlike for passports, the Regulation on identity cards lays down certain rules on the format of the document. It states, firstly, that the specifications set out in part 5 of ICAO Document 9303 apply to the data elements included

<sup>26</sup> Regulation (EU) 2019/1157 of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement [2019] OJ L 188/67.

<sup>27</sup> The explanatory memorandum accompanying the proposal for a regulation states that there are at least 86 different formats of identity cards: Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement SWD(2018) 110, p. 9.

<sup>28</sup> Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals [2002] OJ L 157/1, as amended by Regulation No 2017/1954 [2017] OJ L 286/9.

on identity cards (Article 3(2)) and, secondly, that their format must be consistent with Regulation 1030/2002. Additional technical specifications may be established through the Commission's implementing acts (Article 14). The period of validity is also harmonised: between a minimum of 5 years and a maximum of 10 years (Article 4).

Access to biometric data is only permitted to verify the authenticity of the document and the identity of the holder (Article 11(6)). The Regulation does not stipulate which authorities may access this data as this is to be defined by the Member States. Unlike with the Regulation on passports, Member States must communicate the updated list annually to the Commission for publication purposes (Article 11(7)).

### **3.3. Residence cards of a family member of a Union citizen and permanent residence cards**

Regulation 2019/1157 sets out the uniform format for the residence card by extending the scope of Regulation 1030/2002 on residence permits issued to third-country nationals who do not enjoy free movement rights (Article 7).<sup>29</sup> As far as biometric data is concerned, the residence card must contain a facial image and two fingerprints. Children under the age of 6 years and persons in respect of whom fingerprinting is physically impossible are exempt (Article 4-ter).

Articles 10 and 11 of Regulation 2019/1157, the relevant provisions of which are mentioned in the previous paragraph, also apply to residence cards.

## **4. WHEN AND IN WHAT CONTEXTS BIOMETRIC DOCUMENTS ARE CHECKED**

Directive 2004/38 allows (but does not require) States to check, using documents, the nationality of beneficiaries of free movement of persons when completing the administrative formalities necessary for exercising free movement. But more generally, Union citizens (and their family members) will use their identity documents in their dealings with public or private authorities when carrying out the various formalities that are necessary or useful for living in a complex society. Examples include: dealing with tax authorities, paying taxes, dealing with social security agencies, accessing benefits, dealing with health authorities, receiving healthcare

<sup>29</sup> Article 5 of Regulation 1030/2002 states that it does not apply to third-country nationals who are family members of a Union citizen exercising their right to free movement. However, as the explanatory memorandum accompanying the proposal for a regulation states, some Member States were already using the residence permit format for residence cards.

benefits, dealing with banks, opening and managing a current account, dealing with private individuals, signing a tenancy agreement, and so on and so forth.

Instead, EU law requires national authorities to check documents, including those of Union citizens, at the time of crossing external borders, whether entering or exiting.

Systematic checks on the identity and travel documents of Union citizens at external borders (entering and exiting) was imposed by an amendment to the External Borders Code in 2017.<sup>30</sup> Previously, Union citizens were subject to less detailed checks to ascertain their nationality indicated in their travel document. Systematic checks are carried out when crossing external borders, that is to say those of a Schengen Area State<sup>31</sup> with a third country, when crossing borders between two Member States if internal border controls are still in place,<sup>32</sup> or if such controls have been reintroduced.<sup>33</sup>

This has been prompted by the terrorist threat posed by foreign terrorist fighters, which has brought about changes aimed at restricting the rules in force.<sup>34</sup> The term “foreign terrorist fighters” means nationals of a Member State who had travelled to the Middle East to join ISIS and who, after receiving training, returned to their home State supposedly to commit terrorist attacks. Although some of these individuals were checked when re-entering the European Union, they were not intercepted and went on to commit terrorist acts. The solution devised to counter the threat was to require border guards to carry out systematic database checks on all documents and names of individuals presenting themselves at external borders, whether entering or leaving, putting an end to the more favourable arrangements previously enjoyed by Union citizens.

The new Article 8 of the Borders Code, as amended by Regulation 2017/458, requires national authorities to carry out checks on the documents of all Union

---

<sup>30</sup> Regulation 2017/458 of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders [2017] OJ L 74/1.

<sup>31</sup> Recall that the Schengen Area comprises 26 Member States (with the exception of Ireland) and 4 third countries (Iceland, Liechtenstein, Norway and Switzerland).

<sup>32</sup> This situation occurs in relation to the borders in Bulgaria, (Croatia until March 2023), Cyprus, and Romania.

<sup>33</sup> States may, under certain circumstances and conditions, reintroduce controls at one or more internal borders.

<sup>34</sup> This is very clear from the Commission proposal COM/2015/670. On this phenomenon, see, generally, De Guttry, A.; Capone, F.; Paulussen, C., *Foreign fighters under international law and beyond*, T.M.C. Asser Press, The Hague, 2016; De Coensel, S., *Terrorists on the move: a Legitimacy test of the Criminal Law approach on foreign fighters in Western Europe*, European Criminal Law Review, Vol. 10, No. 2, 2020, pp. 185 - 217.

citizens to verify that they are not counterfeit or stolen, and checks on persons to verify that they do not represent a threat to public policy or national security. To that end, the border guards consult the following databases: SIS II, SLTD (Interpol's Stolen and Lost Travel Documents database), national databases containing information on stolen, misappropriated, lost and invalidated travel documents. Checks on persons are carried out by consulting the SIS and "other relevant Union databases", including national and Interpol databases. Where there are doubts as to the authenticity of the document or the identity of the person, the border guards will verify at least one of the biometric identifiers integrated into the passport in accordance with Regulation 2252/2004. The article goes on to state that "where possible, such verification shall also be carried out in relation to travel documents not covered by that Regulation". This leaves the door open for verification of the biometric identifiers integrated into identity cards under Regulation 2019/1157 (following the 2017 amendment).

The arrangements briefly described above also apply to family members of Union citizens when exercising free movement of persons, in other words when they present themselves at an external border together with a Union citizen or in order to join a Union citizen. In other cases, they are subject to the same rules as third-country nationals, and checks at external borders are also designed to ascertain that they meet the requirements for entering or leaving the Union.

Systematic checks could lead to a refusal of entry. This measure must be justified on the basis of Directive 2004/38, as is evident from the recitals of Regulation 2017/458 (recital 15: "This Regulation is without prejudice to the application of Directive 2004/38/EC of the European Parliament and of the Council"). The Directive applies to the entry of Union citizens into a State of which they are not nationals. But the entry of Union citizens into their country of origin lies outside of its scope.<sup>35</sup>

Entry could be refused for reasons to do with the document or the person. As far as the former is concerned, Article 35 of the Directive allows States to deny any right under the Directive in the case of fraud. As regards the latter, the Directive allows States to restrict rights of entry and residence on grounds of public policy and public security. Any decision restricting one of the free movement rights must be justified by the danger posed by the personal conduct of the individual concerned. In addition, the Directive provides procedural safeguards: any decision restricting free movement rights must be duly substantiated, notified to the individual concerned in writing, and amenable to judicial review.

---

<sup>35</sup> With the exception, which cannot be further discussed here, of Union citizens returning to their country of origin after exercising free movement of persons in another Member State.

However, systematic checks may also lead to other measures, depending on the type of alert that the database search returns. A useful read is the “Practical Handbook for Border Guards”,<sup>36</sup> which outlines how border guards are expected to behave. Of particular interest is the action to be taken for the purposes of discreet or specific checks, pursuant to Article 36 of Council Decision 2007/533/JHA, because it allows border guards to collect further data on persons.

## **5. LEGITIMACY OF COLLECTING, STORING AND PROCESSING BIOMETRIC DATA IN TRAVEL AND IDENTITY DOCUMENTS**

By using biometric data, it is possible to carry out two separate operations: identity authentication and identification. Identity authentication is about ascertaining whether the person holding the document is the same person to whom the document was issued and whose images are stored on the document, by comparing two images: the one on the document and the one taken of the person at that precise moment. This operation does not require the creation of databases but merely offline access to the storage medium placed on the document. Identification is about identifying the biometric data, in other words giving a name and an otherwise unknown identity to the person to whom the biometric data belongs. This operation requires comparing the biometric data to be identified with other biometric data that may be stored in databases.

The basis for each of the operations will be examined separately, relying mainly on primary sources, that is the letter of the relevant EU legislation.

### **5.1. Legitimacy of storing biometric data in documents**

#### **5.1.1. Passports**

The Court of Justice has had the opportunity to rule on the legitimacy of including biometric data in passports,<sup>37</sup> with a preliminary ruling that merits being examined in greater depth.

The national proceedings concerned, on a factual level, the refusal by the competent national authority to issue a passport to the applicant, who refused to have his fingerprints taken, and, from a legal perspective, the validity of Regulation

---

<sup>36</sup> Annex to Commission Recommendation C(2019)7131 establishing a common “Practical Handbook for Border Guards” to be used by Member States’ competent authorities when carrying out the border control of persons and replacing Commission Recommendation C(2006) 5186.

<sup>37</sup> Case C-291/12 *Schwarz* [2013] ECLI:EU:C:2013:670.

2252/2004, in the part where it requires that fingerprints must be taken in order for a passport to be issued. The applicant argues that the Regulation is vitiated by procedural defects (argument rejected by the Court and not of particular interest here) and infringes his fundamental rights. The Court examines this second ground at length and starts from the premise that taking fingerprints constitutes an interference with private life (Article 7 CFREU) and storing them is harmful to the protection of personal data (Article 8 CFREU), since the enjoyment of both rights is restricted (paragraph 30). The Court then considers whether there is a justification for this restriction. Having stated that the consent of the individual concerned cannot be inferred from their application for a passport, because that document is essential for travel (paragraph 32), the Court then goes on to examine the issue through the spectrum of Article 52(1) CFREU,<sup>38</sup> which allows for limitations on fundamental rights provided that a number of conditions are met.

The conditions that the Court considers when assessing whether a limitation of rights is justified are as follows: (a) the limitation must be provided for by law, (b) it must pursue an objective of general interest, (c) it must respect the essence of the rights, (d) it must be proportionate to the objective pursued, and (e) it must be necessary.<sup>39</sup> The Court examines each of these conditions in turn, adopting an approach that is at times vague but nonetheless substantially coherent, which will be summarised here.

(a) A limitation of rights is possible if it is provided for by law, and a regulation is an act that meets that requirement (paragraph 35).

(b) The objective pursued must be one of general interest. Here, the Court does not identify the aim of the regulation directly from the recitals but infers this from the aims that the regulation seeks to pursue. The recitals state that the rules governing biometric passports have two aims: to prevent the falsification of documents and to prevent the fraudulent use of a genuine document. These aims do not seem to fulfil the definition of objectives of general interest. Instead, they are intermediate objectives with respect to the objective that the Court considers to be the general objective recognised by the Union (paragraph 38), namely that of

---

<sup>38</sup> The benchmark for assessing the legitimacy of restricting fundamental rights is therefore primary law. At the time of the ruling, the legislation in force was Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31, which did not contain specific provisions on the processing of biometric data.

<sup>39</sup> This approach is taken from Article 52 CFREU and is consistent with the case law of the Court of Justice. See Lock, T., *Article 52 CFR*, in: Tomkin, J.; Klamert, M.; Kellerbauer, M. (eds.), *EU Treaties and the Charter of Fundamental Rights: Digital Pack: A Commentary*, Oxford University Press, Oxford, 2019

“prevent[ing], *inter alia*, illegal entry into the European Union” (paragraph 37). This general objective seems to this author to be traceable to the legal basis of the Regulation, Article 62(2)(a) TEC, which gave the institutions the competence to adopt measures on the checks to be carried out on persons at external borders, which are certainly not an end in themselves but the means to prevent illegal entry.

(c) According to the Court, which does not elaborate much on this point, the limitation respects the essence of fundamental rights, insofar as the opposite is not proven (paragraph 39).

(d) More detailed are the Court’s discussions on the proportionality of the limitation to the aims pursued, in the sense that this must be appropriate for attaining the aims and must not go beyond what is necessary to achieve them. As regards whether the limitation is appropriate for attaining the specific aims of the regulation, namely to prevent the falsification of documents, the Court answers in the affirmative because this is *in re ipsa*: falsifying a biometric document is undeniably more difficult than falsifying a non-biometric document. In its assessment of the suitability of biometric passports for preventing fraudulent use of a genuine document, the Court discusses the applicant’s argument that the margin of error when comparing fingerprints is too high to conclude that the document is fit for purpose, such that persons fraudulently using a document could be allowed entry and persons using a genuine document could be denied entry (paragraph 42). The Court responds not by contesting the merits of the argument but by minimising its scope: identification mistakes do occur but they are not so serious as to make the document unsuitable. Cases of mismatching do not negate the fact that illegal entries are lower compared with situations where there is no possibility of carrying out checks (paragraph 43). If the fingerprint comparison reveals that the fingerprints do not match, this does not mean that the person concerned will be refused entry but that an additional manual check, as specified in the final sentence of Article 4(3), will be carried out to identify the person concerned and verify their right of entry (paragraph 44). Note that this provision was added by Regulation 444/2009. The original version did not contain any provision to that effect, with all the risks of abuse that this could entail.

(e) The Court then states that the limitation of fundamental rights is necessary insofar as it does not go beyond what is necessary to achieve the aim, since fingerprinting is not an operation of an intimate nature (paragraph 48). In addition, measures that are equally effective and interfere less with the rights protected are not available. The only measure that can be considered is iris recognition, a procedure that the Court considers equivalent in terms of interference with rights at the time of the image is collected, but less effective in preventing fraudulent use

of passports, because the technology required is more expensive and the margin of error is no lower than for fingerprints (paragraph 52). Finally, the processing of fingerprints stored in the document must not go beyond what is necessary to achieve the aim pursued. According to Article 4(3) of the Regulation, the legitimate use of fingerprints is strictly limited to the aims pursued (verifying the authenticity of the passport and the identity of the holder) and is restricted to authorised staff.

### 5.1.2. Identity cards

The Court of Justice has not yet had the opportunity to rule on the legitimacy of collecting, storing and using fingerprints in identity cards and residence cards, although a number of references for a preliminary ruling are pending.<sup>40</sup>

To attempt an answer, it is possible to apply the same arguments developed by the Court in *Schwarz* as regards passports to identity cards and examine whether legitimacy can be based on consent or on the existence of grounds for justification for interference with fundamental rights under Article 52 CFREU.

Consent cannot form the basis for interference, because possession of an identity card is compulsory in almost all States and the applicant cannot choose whether or not to apply for one. If the Court has stated that consent cannot be presumed from a passport application, the same applies to an identity card.

Considering instead the arguments based on Article 52 CFREU, it can be stated first and foremost that interference is provided for by law, as this is specified in a regulation.

As regards the objective of general interest recognised by the Union, it seems difficult to argue that the objective identified by the Court for passports, namely to prevent unlawful entry into the EU, can also apply to identity cards. This is because there is nothing in the legal basis of the Regulation that concerns the control of external borders. Unlike Regulation 2252/2004, which is based on Article 62(2)(a) TEC, now corresponding to Article 77 TFEU, Regulation 2019/1157 finds its legal basis in Article 21(2) TFEU. This article allows the institutions to adopt provisions to facilitate the exercise of rights connected with the free movement of persons, in the absence of any other legal basis. The choice of this legal basis deserves some consideration. At first glance, it may be assumed that there is another, more suitable provision, Article 77(3), which authorises the institutions, once again in the absence of a more appropriate legal basis, to adopt provisions

---

<sup>40</sup> Cases C-61/22 [2022] OJ C 213/22, and C-280/22 [2022] OJ C 318/22.

concerning identity cards and passports which are necessary for the exercise of the rights referred to in Article 20(1) (i.e. free movement).<sup>41</sup> The exact scope of the two provisions is not self-evident. From a procedural point of view, the choice between the two provisions is not without consequences. Article 77 falls within the Area of Freedom, Security and Justice, and acts adopted on this basis are not binding on Denmark and Ireland.<sup>42</sup> In addition, Article 77(3) provides that the Council shall act unanimously after consulting the European Parliament, in accordance with a special legislative procedure in which the role of the Parliament is less incisive than under the ordinary legislative procedure provided for in Article 21(2).<sup>43</sup>

Moreover, an identity card, unlike a passport, is not primarily a travel document. It performs the function of a travel document only for travel between Member States, for entry into a Member State from a third country, and for exit into third countries with which agreements have been concluded under which an identity card can be accepted as a travel document. Although the recitals specify that identity cards have a predominantly internal function, it is also true that the genesis of the regulation can seemingly be explained by considering its function as a travel document. Recital 13 states that identity cards that are not travel documents do not fall within the scope of the regulation. The regulation on passports is the foundation on which Regulation 2019/1157 is clearly built. Biometric data does not seem to be so essential in enhancing the document's function of identifying the holder, if it is considered that States can continue to accept documents other than travel documents for proof of identity (recital 12), such as driving licences, which do not contain biometric data. Somewhat absurdly, a document that does not contain biometric data could be used to confirm the holder's identity in the event of a mismatch.

The purpose of Regulation 2019/1157 is then specifically identified. The objective, inherent in its legal basis, is to facilitate the free movement of persons. Recital 17 states that “[t]he inclusion of [...] biometric indicators [should] allow Union citizens to fully benefit from their rights of free movement”. Given the importance of free movement of persons under EU law, this can easily be considered an ob-

---

<sup>41</sup> Doubts are raised as to the appropriateness of the legal basis, although without going into the reasons, in Quintel, T., *The Commission Proposal and EDPS Opinion 7/2018 on the Proposed Regulation concerning Identity Cards and Other Documents*, *European Data Protection Law Review*, Vol. 4, No. 4, 2018, p. 510.

<sup>42</sup> Articles 1 and 2 of Protocol (No. 22) on the position of Denmark. Articles 1 and 2 of Protocol (No. 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice.

<sup>43</sup> The ordinary legislative procedure is considered more democratic and abstractly more preferable. However, it is settled case-law that the choice of procedure does not guide the choice of legal basis, but rather it is the legal basis that determines the procedure to be followed.

jective of general interest of the Union. Therefore, it is the necessity and proportionality of the collection and storage of biometric data that requires explanation.

The recitals to the Regulation state that identity cards and residence cards are among the most frequently falsified documents. This is not surprising, given the importance of proving one's status as a beneficiary of the right of free movement. Directive 2004/38 indirectly legitimises measures to combat falsification by allowing States to sanction the use of counterfeit documents by refusing the rights of residence applied for or by revoking rights previously granted. The point is to understand how the enhanced security of identity cards resulting from the inclusion of biometric data facilitates free movement. The explanatory memorandum accompanying the Commission's proposal contains a number of provisions, not included in the final regulation, which are enlightening: "secure identity cards and residence documents are essential elements to ensure the trust needed for free movement within an area of freedom and security" and "citizens can [...] not rely on their documents to exercise their rights if they cannot be sure that their documents will be accepted outside their Member State(s) of issuance". This assertion does not however appear to be supported by substantial evidence. True, there is anecdotal evidence of identity cards not being accepted and of a number of EU citizens experiencing difficulties when dealing with the public administration or with private parties because of identity cards not being accepted as proof of citizenship. But it does not seem immediately apparent that these difficulties are indicative of a structural problem requiring legislative intervention on a scale similar to that which happened for Regulation 2019/1157. Indeed, it would be possible to envisage a uniform model of identity card with advanced security features even without two types of biometric data.

Including biometric data in identity documents could facilitate free movement if it served to avoid or minimise the checks to which Union citizens would otherwise be subject. However, no proof of this is given.

Therefore, it does not appear that the regulation in question is pursuing an objective of general interest, considering its legal basis, such as to justify the limitation of fundamental rights arising from the taking and storage of fingerprints in identity cards. But even in the event that the proposed interpretation were not considered acceptable and that the objective pursued (whatever it may be) were considered one of general interest, the proportionality and necessity test would have to include, unlike what happened in *Schwarz*, an additional factor, namely the huge number of persons involved (all citizens of States where identity cards are compulsory, plus citizens of States where identity cards are not compulsory, if they apply for one) and the variety of circumstances in which an identity card must be

presented. In this context, false negatives or positives are likely to be particularly substantial in absolute value and therefore deserving of proper attention.<sup>44</sup>

### 5.1.3. Residence cards

The comments made in the previous section also apply to the legitimacy of collecting and storing biometric data in residence cards, albeit that a number of clarifications are required. Firstly, a residence card is neither an identity document nor a travel document. However, possession of a residence card exempts the holder from the requirement to hold a visa to enter a Member State from another Member State or from a third country. This function is to do with immigration management and prevention and control of unlawful immigration, with the result that the objective of general interest pursued with biometric passports can plausibly be extended to residence cards. However, the choice of Article 21(2) as the proper legal basis is debatable.

## 5.2. Storage and processing of biometric data for identification purposes

In *Schwarz*, the appellant then feared a further risk, which would have invalidated Regulation 2252/2004, namely the storage, centrally, of fingerprints collected in accordance with the Regulation and the use thereof for purposes other than authorised purposes. The Court acknowledges the existence of the risk, which is inherent in the use of fingerprints to identify persons, but considers this unfounded in this particular case, because the Regulation legitimises only the storage of fingerprints in the document, which remains in the holder's possession. Moreover, the Regulation cannot be interpreted as justifying the central storage of data or the use of such data for other purposes (paragraph 61). Once again, an important amendment is made by Regulation 444/2009, which adds a recital containing this principle and which is considered by the Court to be an interpretative principle that limits - or rather prevents - any extensive interpretation of the Regulation.

The Court returns to the subject of central storage and use of fingerprints in its judgment in the subsequent *Willems* case.<sup>45</sup> The case in question raises similar questions to those in *Schwarz*. The referring court asked the Court of Justice to interpret the Regulation as opposed to considering its validity. Of interest here is the Court's answer to the referring court's question on the interpretation of the Regulation as a basis for legitimising the storage of fingerprints in national databases. The national court asks whether Regulation 2252/2004, read in the light

<sup>44</sup> Quintel, T., *op. cit.* note 41, also highlights the increased risk of lost or stolen documents, p. 511.

<sup>45</sup> Joined Cases C-446/12 to C-449/12 [2015] ECLI:EU:C:2015:238.

of the Charter of Fundamental Rights, “must be interpreted as meaning that it requires Member States to guarantee that the biometric data collected and stored pursuant to that regulation will not be collected, processed and used for purposes other than the issue of passports or other travel documents.” (paragraph 43). The Court reiterates the principle previously expressed in *Schwarz*, and takes it to its logical conclusion: the Regulation does not authorise the central storage of data or its subsequent use, but neither does it prohibit it. The Charter of Fundamental Rights is therefore the benchmark for assessing the legitimacy of States’ conduct only if they act within the scope of EU law, which does not apply in the case in question. But the Court adds a rather frequent *obiter dictum*, acting *ultra petitum* and *ultra vires*, insofar as it does not look at the law which it is competent to interpret, but points out the obvious, not such much to the national court, because the question is hypothetical, as to all national legislative, administrative and judicial authorities: any State decision regarding the central storage or subsequent use of data would not escape judicial review by the national courts, to be conducted in the light of national law and, if appropriate, of the ECHR (paragraph 51). The Court does not examine the question in the light of Directive 95/46, which was in force at the time, because the referring court did not request an interpretation of that Directive.

The Court of Justice has made it abundantly clear that the regulations cannot justify a different use of the data. Regulation 2019/1157 is more explicit than Regulation 2252/2004 and requires the destruction of fingerprints once the document is handed over to the holder, but adds the sentence “Other than where required for the purpose of processing in accordance with Union and national law” (Article 10(3)).

Therefore, whether the Union or the Member States can use the data collected for other purposes is a question that cannot be resolved on the basis of the regulations relating to biometric documents. Given that States will be collecting a huge amount of photos and fingerprints, namely those of all their citizens (in States where the possession of an identity card is compulsory and of passport holders in States where it is not), it is not hard to imagine that States might also want to use them for other purposes (e.g. for police purposes or for preventing crime or fraud against State finances) and that question marks might be raised over that conduct.

The question of the legitimacy of the storage and processing of biometric data must therefore be addressed. Under EU law, biometric data is personal data if it is used to identify a person uniquely. The processing of such data is governed by three different Union acts: Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement

of such data;<sup>46</sup> Directive 2016/680 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;<sup>47</sup> and Regulation 2018/1725 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.<sup>48</sup>

All of these acts define biometric data in the same way,<sup>49</sup> i.e. as personal data, the processing of which is governed by those acts, if it is processed in such a way as to allow or confirm the unique identification of a person. The rules on processing differ according to the purpose. For purposes relating to judicial cooperation in criminal matters and police cooperation, “the processing of [...] biometric data for the purpose of uniquely identifying a natural person” is possible “only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law” (Article 10 of Directive 2016/680). Article 76 of Regulation 2018/1725 is worded similarly: “Processing of [...] biometric data for the purpose of uniquely identifying a natural person [...] shall be allowed only where strictly necessary for operational purposes, within the mandate of the Union body, office or agency concerned and subject to appropriate safeguards for the rights and freedoms of the data subject”. For different purposes, processing is prohibited, unless exceptions apply, including: “the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject”.<sup>50</sup> According to Article 9(4) of Regulation 2016/679, Member States

---

<sup>46</sup> Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1.

<sup>47</sup> Directive 2016/680 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 [2016] OJ L 119/89.

<sup>48</sup> Regulation 2018/1725 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 [2018] OJ L 295/39.

<sup>49</sup> Article 4(14) of Regulation 2016/679; Article 3(13) of Directive 2016/680; Article 3(18) of Regulation 2018/1725. For an analysis of Article 4(14) of Regulation 2016/69, see Jasserand, *op. cit.* note 18, as well as Bygrave, L.; Tosoni, L., *Article 4(14). Biometric data*, in: Kuner, C.; Bygrave, L.; Docksey, C.; Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020.

<sup>50</sup> Article 9(2)(g) of Regulation 2016/679. And also Article 10(2)(g) of Regulation 2018/1725.

may introduce further conditions including limitations. Where an exception applies, processing must still comply with the general conditions specified<sup>51</sup>.

As legal scholars have highlighted, the processing of biometric data is regulated if it serves to identify the person, whereas processing for authentication or verification of a person's identity is not covered,<sup>52</sup> as this is an operation that is essentially carried out using the biometric data stored in identity documents.

Thus, analysing the relevant EU acts reinstates the possibility of collecting and processing biometric data for the purpose of uniquely identifying a person, albeit within strict limits to be carefully justified. On the other hand, it seems to exclude the possibility of interpreting these rules as prohibiting States or the Union from establishing such databases.

## 6. CONCLUDING REMARKS: DATABASES AND INTEROPERABILITY

The legitimacy of the collection and storage of biometric data, which the Court of Justice has addressed and resolved in its case law, should not be considered in isolation but rather placed within the broader debate on databases established by the Union or by Member States. On the one hand, it is evident that the databases established by the European Union have multiplied in number in recent years and many of them collect biometric data.<sup>53</sup> As legal scholars have pointed out, this is a form of cooperation between national authorities which is appreciated by States.<sup>54</sup> On the other hand, in more recent times, the Union has been pursuing the goal of

<sup>51</sup> Article 6 of Regulation 2016/679, Article 5 of Regulation 2018/1725. Georgieva, L.; Kuner, C., *Article 9. Processing of special categories of personal data*, in: Kuner; Bygrave; Docksey; Drechsler (eds.), *op. cit.* note 49.

<sup>52</sup> Bygrave, L.; Tosoni, L., *op. cit.* note 49.

<sup>53</sup> EU databases are widespread in the area of immigration, where they are used to manage visa policy and international protection policy (EES, ETIAS, EURODAC, VIS) and in the area of police cooperation (ECRIS, SIS). Rijpma, J., *Brave New Borders: The EU's Use of New Technologies for the Management of Migration and Asylum*, in: Cremona, M. (ed.), *New Technologies and EU Law*, Oxford University Press, Oxford, 2017, pp. 197 - 238.

Third-country nationals are now subject to a kind of mass data gathering. Indeed, records are kept of any third-country national entering the Union legally or illegally, whether they require a visa (VIS), do not require a visa (ETIAS or EES), are applying for international protection or are apprehended at external borders (EURODAC). There is plentiful discussion about whether such data gathering is lawful and whether it breaches the principle of non-discrimination on the basis of nationality, since EU citizens are not subject to the same measures. However, the discussion is following a strange course because instead of restricting data gathering in relation to third-country nationals, the trend is to intensify this in relation to Union citizens.

<sup>54</sup> Brito Bastos, F.; Curtin, D.M., *Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue*, *European Public Law*, 2020, Vol. 26, No. 1, pp. 59 - 70, p. 60 et seq.

making databases interoperable, so as to make better use of the information they contain.<sup>55</sup> Interoperability connects different databases and makes the data stored in them searchable and accessible to a wider range of authorities and for different purposes from those for which the data is collected. A single search should be possible in all databases that the operator is authorised to access. So databases that are set up as independent and pursue a specific purpose (purpose limitation principle) may also be searched by different persons and for different purposes from those originally intended. Although this may be justified on the basis of the law, it represents a paradigm shift, which is more than the simple sum of its parts and cannot be considered legitimate simply because its individual components are legitimate. A change of this kind is a step towards widespread control that foreshadows a worrying society which, above all, is not the consequence of a conscious and democratically made political choice<sup>56</sup> but rather the collateral effect of administrative cooperation.

## REFERENCES

### BOOKS AND ARTICLES

1. Abeyratne, R.I.R., *The Development of the Machine Readable Passport and Visa and the Legal Rights of the Data Subject*, *Annals of Air and Space Law*, Vol. 17, Part 2, 1992, pp. 1 – 24
2. Baechler, S., *Document Fraud: Will Your Identity Be Secure in the Twenty-first Century?*, *European Journal on Criminal Police and Research*, Vol. 26, 2020, pp. 379 – 394
3. Brito Bastos, F.; Curtin, D.M., *Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue*, *European Public Law*, Vol. 26, No. 1, 2020, pp. 59 – 70
4. Bygrave, L.; Tosoni, L., *Article 4(14), Biometric data*, in: Kuner, C.; Bygrave, L.; Docksey, C.; Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020
5. De Coensel, S., *Terrorists on the move: a Legitimacy test of the Criminal Law approach on foreign fighters in Western Europe*, *European Criminal Law Review*, Vol. 10, No. 2, 2020, pp. 185 – 217
6. De Guttry, A.; Capone, F.; Paulussen, C., *Foreign fighters under international law and beyond*, T.M.C. Asser Press, The Hague, 2016

<sup>55</sup> For an overview of the problems that interoperability poses, see the essays collected in the Special Issue cited in the previous footnote.

<sup>56</sup> Gonçalves, M.E.; Gameiro, M.I., *Does the Centrality of Values in the Lisbon Treaty Promise More Than It Can Actually Offer? EU Biometrics Policy as a Case Study*, *European Law Journal*, Vol. 20, No. 1, 2014, pp. 21 - 33 point out not only that biometric passports were adopted without discussion within civil society, but also that the decision to adopt them was motivated by the advantages to be gained from collecting biometric data, whereas the impact that this may have on individual freedom and democracy was not considered. Herting Randall, Hänni, *op. cit.*, note 16, at par. 18, point out that the establishment of central databases of biometric data “would undermine the symbolic value of the European Passport, turning it from a symbol of a common, right-based identity into a threat to civil liberties.”

7. Georgieva, L.; Kuner, C., *Article 9. Processing of special categories of personal data*, in: Kuner, C.; Bygrave, L.; Docksey, C.; Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020
8. Gonçalves, M.E.; Gameiro, M.I., *Does the Centrality of Values in the Lisbon Treaty Promise More Than It Can Actually Offer? EU Biometrics Policy as a Case Study*, *European Law Journal*, Vol. 20, No. 1, 2014, pp. 21 - 33
9. Guild, E.; Peers, S.; Tomkin, J. (eds.), *The EU citizenship directive: a commentary*, Oxford University Press, Oxford, 2<sup>nd</sup> ed., 2019
10. Hagedorn, C., *Passport*, Max Planck Encyclopedia of Public International Law, 2008
11. Herting Randall, M.; Hänni, D., *European Passport*, Max Planck Encyclopedia of Public International Law, 2019
12. Hornung, G., *Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues*, *European Public Law*, Vol. 11, 2005, pp. 501 – 514
13. Jasserand, C., *Legal Nature of Biometric Data: From ‘Generic’ Personal Data to Sensitive Data*, *European Data Protection Law Review*, Vol. 2, No. 3, 2016, pp. 297 - 311
14. Lock, T., *Article 52 CFR*, in: Tomkin, J.; Klamert, M.; Kellerbauer, M. (eds.), *EU Treaties and the Charter of Fundamental Rights: Digital Pack: A Commentary*, Oxford University Press, Oxford, 2019
15. Quintel, T., *The Commission Proposal and EDPS Opinion 7/2018 on the Proposed Regulation concerning Identity Cards and Other Documents*, *European Data Protection Law Review*, Vol. 4, No. 4, 2018, pp. 505 – 514
16. Rijpma, J., *Brave New Borders: The EU’s Use of New Technologies for the Management of Migration and Asylum*, in: Cremona, M. (ed.), *New Technologies and EU Law*, Oxford University Press, Oxford, 2017, pp. 197 – 238
17. Torpey, J., *The invention of the passport: surveillance, citizenship, and the state*, Cambridge University Press, Cambridge, 2018

## **COURT OF JUSTICE OF THE EUROPEAN UNION**

1. Case C-376/89 Giagounidis [1991] ECLI:EU:C:1991:99
2. Case C-459/99 MRAX [2002] ECLI:EU:C:2002:461
3. Case C-157/03 Commission v Spain [2005] ECLI:EU:C:2005:225
4. Case C-215/03 Oulane [2005] ECLI:EU:C:2005:95
5. Case C-291/12 Schwarz [2013] ECLI:EU:C:2013:670
6. Joined Cases C-446/12 to C-449/12 [2015] ECLI:EU:C:2015:238
7. Case C-101/13 U [2014] ECLI:EU:C:2014:2249
8. Case C-202/13 McCarthy [2014] ECLI:EU:C:2014:2459
9. Case C-246/17 Diallo [2018] ECLI:EU:C:2018:499
10. Case C-754/18 Ryanair Designated Activity Company [2020] ECLI:EU:C:2020:478
11. Case C-35/20 A [2021] ECLI:EU:C:2021:813
12. Case C-490/20 Stolichna obshtina, rayon ‘Pancharevo’ [2021] ECLI:EU:C:2021:1008

13. Case C-61/22 [2022] OJ C 213/22, Landeshauptstadt Wiesbaden, pending
14. Case C-280/22 Kinderrechtencoalitie Vlaanderen and Liga voor Mensenrechten [2022] OJ C 318/22, pending

## **EU LAW**

1. Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals [2002] OJ L 157/1
2. Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L 385/1
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31
4. Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC [2004] OJ L 158/77
5. Directive 2016/680 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 [2016] OJ L 119/89
6. 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 [2009] OJ L 142/1
7. Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1
8. Regulation 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders [2017] OJ L 74/1
9. Regulation 2018/1725 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 [2018] OJ L 295/39
10. Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement [2019] OJ L 188/67