ISSN 2384-9169
Fascicolo n. 3 - 2020
rivista.eurojus.it

Information sharing of data related to cross-border movement: travellers and migrants' data protection*

Summary: 1. Introduction. – 2. The regulatory framework of the data acquisition, the data retention and the information sharing related to the third-country citizens, travellers and migrants. – 3. Migrants and travellers' data protection according to the current regulatory framework and its shortcomings. – 4. Recent developments in the border management policy and in the safeguard of TCNs' data protection and some final considerations.

1. Introduction

In the last decade, two trends are emerging parallel to one another: i) the urgent need to join up and strengthen in a comprehensive manner the EU's information tools for border management, migration and security and ii) the development of the legal framework concerning the respect of fundamental rights including, in particular, the right to the protection of personal data.

On the one hand, the fighting of crimes related to terrorism and of illegal migration has brought a stronger attention to the cross-border regular and irregular movements. For this purpose, some systems collect personal data of regular and irregular migrants and also of travellers, both EU and non-EU citizens.

On the other hand, the European Charter of Fundamental Rights protects the right to the respect of private life and the right to the protection of personal data (art. 7 and 8). Moreover, in 2012 the reform of the EU's data protection rules has begun, through the adoption of a general Regulation on data protection[1] and of a specific Directive[2] on data protection in the area of police and justice, both applicable as of May 2018. Furthermore, in *Digital Rights Ireland* the

*Assegnista di ricerca in Diritto dell'Unione europea, Università Federico II, Napoli.

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

[2] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119.

European Court of Justice (hereinafter: ECJ) declared invalid a directive that established data retention insofar as it exceeded the limits imposed by the principles of proportionality and necessity.

According to the current regulatory framework, three main systems govern the data acquisition, the data retention, and the information sharing related to the third-country citizens, travellers and migrants and a fourth has been recently introduced. In the subsequent paragraph an explanation of each database will be provided, defining the purpose of the data collection and sharing and the authorities authorized to access the data. Afterwards (par. 3), it will be examined whether an effective data protection is actually guaranteed.

Finally, the article will focus on the recent developments of these systems (par. 4). Two recent regulations establish a framework for interoperability between EU information systems, aiming at better protecting EU's external border, strengthening internal security and improving the management of migration. All the information systems will be managed by four new interoperability components that will allow the detection of multiple identities and will counter identity fraud. It will be evaluated whether the massive data collection and the enhancement of the information systems and information sharing fulfil the necessity and proportionality requirements and whether the data of the third-country travellers and migrants are effectively protected.

2. The regulatory framework of the data acquisition, the data retention and the information sharing related to the third-country citizens, travellers and migrants

The establishment of the Schengen area, according to the Schengen Agreement of 1985 and its subsequent amendments, has enabled the creation of a territory without internal borders where the free movement of persons is guaranteed. The signatory States have introduced a single external border and, simultaneously, they have set down common rules and procedures for visas for short stays, asylum requests and border controls.

Right from the beginning, according to the Convention of 19 June 1990 implementing the Schengen Agreement, the Schengen Information System (hereinafter: SIS) was born. At the heart of the SIS, an information system was set up to enable national border control and judicial authorities to obtain information on persons or objects. This system has evolved into the SIS II, which has recently been replaced by new SIS Regulations[3], and it constitutes a compensatory measure contributing to maintaining a high level of security within the area of freedom, security

[3] The second generation of the Schengen Information System entered into operation on 9 April 2013 on the basis of Regulation 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II). This regulation has been repealed by Regulation 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement (hereinafter SIS Regulation), OJ L 312, as amended by Regulation 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration […], OJ L 135.
See also Regulation 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, OJ L 312 and Regulation 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters[…], OJ L 312, as amended by Regulation (EU) 2019/818, cited.

and justice (AFSJ) of the EU. Through this system the conditions and the procedures for entry are established, as well as the procedures for the processing and the exchange of a broad spectrum of alerts in respect of third-country nationals (hereinafter: TCN) for the purpose of refusing entry into, or a stay in, a Member State.

An alert shall be inserted in the SIS on the basis of a decision taken, on the basis of an individual assessment, by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law[4]. The issuing of an alert shall be based on a threat to public policy or public security or to national security which the presence of the third-country national in question in the territory of a Member State may pose. For this purpose, according to art. 24 of SIS Regulation, such a threat arises when a TCN i) has been convicted in a Member State of an offence carrying a penalty involving the deprivation of liberty of at least one year; ii) there are serious grounds for believing that he has committed a serious criminal offence, including a terrorist offence, or there are clear indications of his or her intention to commit such an offence in the territory of a Member State; or iii) has circumvented or attempted to circumvent Union or national law on entry into and stay on the territory of the Member States.

The alert is composed of several pieces of information: personal data such as name at birth and previously used names and any aliases, place and date of birth, nationality, sex, and any specific, objective, physical characteristics not subject to change; biometric data such as photographs and fingerprints; personal information related to the alert like the authority issuing the alert, the type of offence, the reference to the decision giving rise to the alert, reason for the alert, whether the person concerned is armed, violent or has escaped and action to be taken[5].

Access to this information is currently accorded, first of all, to authorities responsible for the identification of third-country nationals for the purposes of border control, in accordance with the Schengen Borders Code[6].

Moreover, the SIS database can also be consulted by other police and customs checks carried out within the concerned Member State and by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge, as provided for in national legislation[7].

The SIS is the most widely used law enforcement information-sharing instrument today, and it is considered complementary to the other centralised systems in the managing of borders, migration, visa processing and asylum, and in fighting crime and terrorism. The other existing centralized information systems of data acquisition related to the migration policies are VIS,

---

4 Member States supply information to the system through national networks (N-SIS) connected to a central system (C-SIS). This IT system is supplemented by a network known as SIRENE (Supplementary Information Request at the National Entry), which is the human interface of the SIS.

5 See art. 20 of SIS Regulation, cit.

6 Regulation 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) as amended by Regulation 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa […], OJ L 135.

7 All the authorities that can have access to the SIS shall be included in a list: according to art. 41, para. 8, SIS Regulation, each Member State shall send to eu-LISA a list of its competent authorities authorised to search directly the data contained in SIS II pursuant to this Regulation as well as any changes to the list. That list shall specify, for each authority, which data it may search and for what purposes. eu-Lisa shall ensure the annual publication of the list in the OJ.

EES and Eurodac and these systems are more strictly related to the Common visa policy and migration policy.

The common visa policy is considered a part of the Schengen *acquis* and is composed by a *corpus* of detailed provisions and practical procedures adopted for the release of visas for transit through or intended stays in the territory of the Member State not exceeding three months in any six-month period[8]. These rules aim at facilitating legitimate travel and tackling illegal immigration.

According to the Seville European Council, the common visa policy was to be completed by the establishment of a common identification system for visa data (hereinafter: VIS). For this purpose, Decision 512/2004 was adopted[9], enabling authorised national authorities to enter and update visa data and to consult these data electronically. Afterwards, Regulation 767/2008 has defined the conditions and procedures for the exchanging of data between Member States[10] and Council Decision 2008/633/JHA has specified the conditions for the access for consultation of VIS by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences[11].

The VIS data base contains different kinds of data: personal data such as surname, first name, nationality, date and place of birth, sex, photography and fingerprints; information related to the travel but that is also personal information, like main purpose of the journey, State of first entry, dates of arrivals and departure, applicant's home address, current occupation or educational establishment and data related to the liability to pay the applicant's subsistence costs during the stay[12].

These data are, firstly, collected to facilitate the fight against fraud in visa application and to ease checks at external border crossing points. Moreover, the information collected in the VIS allows the combat of irregular migration permitting the identification of persons who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member.

Furthermore, VIS can be used to combat terrorism and other serious criminal offences, contributing to the prevention of threats to the internal security of the Member States. For this purpose, the designated authorities of the Member State may, in a specific case and following

---

8 Regulation 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), as amended by Regulation 2019/1155 of the European Parliament and of the Council of 20 June 2019 amending Regulation 810/2009 establishing a Community Code on Visas (Visa Code), OJ L 188.

9 Council Decision of 8 June 2004, no. 512, establishing the Visa Information System (VIS), OJ L 213, as amended by Regulation 2019/817, cited. The cited Decision introduces a legal basis for the creation of a system based on a central information system (hereinafter CS-VIS) and an interface in each Member State (hereinafter NI-VIS

10 Regulation 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, as amended by Regulation 2019/817, cited.

11 Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, as amended by Regulation 2019/817, cited. About the VIS see, between the others, S. PEERS, *Legislative Update, EC Immigration and Asylum Law: The New Visa Code*, in *European Journal of Migration and Law*, 2010, p. 105 ss.

12 See art. 9 of VIS Regulation. In the VIS will be also entered data related to the visa application, the visa issuing or for a visa refusal, see Art. 8 seq.

a reasoned written or electronic request, access the data kept in the VIS according to the rules established by Decision 2008/633/JHA. Following the opinion given by the European Personal Data Supervisor (hereinafter: EPDS or Data Supervisor) concerning the Commission proposal on the institution of VIS[13], Decision 2008/633/JHA defines the conditions for access, with the aim that the Member State's designed Authorities can obtain access to the VIS data only on a case-by-case basis and excluding routine access[14]. These conditions are fundamental to guarantee limited access to the personal data of the Visa applicants, connected to a specific event or to a danger associated with serious crime. As we will see hereinafter, these conditions assure the respect of the proportionality and necessary requirements in the use of personal data. Nonetheless there are still some doubts about the accomplishment of the data protection right.

According to art. 17*a* of the VIS Regulation, an interoperability between the VIS and the Entry/Exit System (hereinafter: EES) has been established, created by Regulation 2017/2226[15]. The EES has introduced a database for the recording and storage of the date, time and place of entry and exit or of a refusal of entry of TCN crossing the borders of the Member States. This system also calculates the duration of the authorised stay of such third-country nationals and generates an alert to the Member State when the authorised stay has expired.

The objectives of the EES are three: improving the management of external borders, preventing illegal immigration and facilitating the management of migration flows. This system, indeed, contributes to the identification of any person who does not fulfil or no longer fulfils the conditions of duration of the authorized stay on the territory of a Member State. The new system has improved the previous slow and unreliable practice of manual stamping of passports[16]. Moreover, the EES should be used for the prevention, detection and investigation of terrorist offences and of other serious criminal offences[17]. For this purpose, according to art. 29 of the EES Regulation, Member States shall designate the authorities which are entitled to consult the EES data.

Just like the VIS, the EES also operates through a Central System and the National Uniform Interface (NUI) in each Member State, enabling the connection of the EES Central System to the national border infrastructures. The EES Central System is hosted by eu-LISA in its technical sites, which shall also establish a Secure Communication Channel between the EES Central System and the VIS Central System to enable interoperability between the EES and the VIS.

---

13 Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM(2004)835 final), OJ 2005, C 181.

14 According to Art 3 of VIS Regulation, cit., access for consultation must be a) necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences; b) necessary in a specific case; c) supported by reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question.

15 Regulation 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations 767/2008 and 1077/2011, OJ L 327, as amended by Regulation 2019/817, cited.

16 See whereas 15 e art. 6 of EES Regulation, cit. The EES has been created also to combat identity fraud and the misuse of travel documents.

17 See art. 1, para 2, of EES Regulation, cit.

While VIS and EES have as first purpose data collection and sharing to prevent the illegal obtaining of a visa and an illegal stay over a short period, the Eurodac system[18] has been established to collect and transmit fingerprint data of asylum applicants and third-country nationals who have crossed the external borders irregularly or who are illegally staying in a Member State. Like the other systems, Eurodac was created to manage the migration flow, in particular assisting Member States in application of the Dublin regulation[19], but it is also available for the comparison of fingerprint data for prevention, detection or investigation of terrorist or other serious criminal offences.

According to the Eurodac Regulation, each Member State shall promptly take the fingerprints of all fingers of every applicant for international protection of at least 14 years of age and of who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country[20].

The fingerprints will be inserted in the database with the indication of the Member State of origin, place and date of the application for international protection, sex and reference number of the migrant used by the Member State of origin. The Operator also has to insert his ID and the dates of the fingerprint collection and transmission.

For a correct application of the Dublin Regulation, the Eurodac can be requested in order to check whether a TCN or a stateless person found illegally staying within its territory has previously lodged an application for international protection in another Member State. Nonetheless, the system is also available by Member State' designated authorities responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences[21]. The Eurodac Regulation establishes several conditions for access to Eurodac by designated authorities: the authority can submit a reasoned electronic request only after an unsuccessful comparison with the national fingerprint databases and VIS. Moreover, the comparison has to be necessary for the purpose and in the specific case and there are reasonable grounds to consider that the comparison will substantially contribute to the purpose. The national Authority shall ensure that the conditions for requesting comparisons of fingerprints with Eurodac data are fulfilled.

All the systems described above are centralised systems of collection and sharing data related to travellers and migrants, and all the information collected is managed by the European agency eu-Lisa[22].

---

18 Regulation 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of Regulation 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, OJ L 180.

19 Regulation 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, OJ L 180.

20 See art. 9 and 14 of EURODAC Regulation, cit.

21 According to art. 5 of Eurodac Regulation, cit., designated authorities shall not include agencies or units exclusively responsible for intelligence relating to national security.

22 Regulation 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), OJ L 295, as amended by Regulation 2019/817, cited.

In this context, it is also important to highlight the national information systems and decentralised EU information systems related to the acquisition of travellers' data, like Advance Passenger Information (hereinafter: API) and the Passenger Name Record (hereinafter: PNR). They are also relevant considering that Member States should exchange the information among each other through relevant information exchange networks and ensure interoperability.

The API Directive[23] regulates the transfer of advance passenger information data by air carriers to the competent national authorities for the purpose of improving border controls and combating illegal immigration. The transmitted information is personal data like full name, date of birth, nationality, number and type of travel document used and information related to the travel like the border crossing point of entry into the territory of the Member State, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport, and the initial point of embarkation.

According to Art. 6, the personal data shall be communicated to the authorities responsible for carrying out checks on persons at external borders through which the passenger will enter the territory of a Member State, for the purpose of facilitating the performance of such checks and with the objective of combating illegal immigration more effectively. After passengers have entered, these authorities shall delete the data within 24 hours after transmission. However, these data can be retained if they "are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders in accordance with national law and subject to data protection provisions under Directive 95/46/EC"[24]. This provision could rise doubts as to its compliance with the right to the protection of personal data, even if in this case the Member State has to respect the data protection legal framework established by Regulation 2016/679 and Directive 2016/680.

Travellers' data is also collected (and shared) in accordance with the PNR Directive[25]. The Annex I to the PNR Directive lists a large amount of information related to the traveller and his journey[26] and every Passenger Information Unit (PIU, designed by the Member State)

---

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

24 Despite the national authorities, the carriers are obliged to delete, within 24 hours of the arrival of the means of transportation, the personal data they have collected and transmitted to the border authorities for the purposes of this Directive.

25 Directive 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119.
About the PNR Directive see, between the others F. GALLI, *Passenger Name Record Agreements: The Umpteenth Attempt to Anticipate Risk*, EUCRIM, 2010, p. 124 ss.

26 According to Annex I to the PNR Directive, the Passenger name record data are: PNR record locator; Date of reservation/issue of ticket; Date(s) of intended travel; Name; Address and contact information; All forms of payment information, including billing address; Complete travel itinerary for specific PNR; Frequent flyer information; Travel agency/travel agent; Travel status of passenger, including confirmations, check-in status, no-show or go-show information; Split/divided PNR information; General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent); Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields; Seat number and other seat information; All baggage information; Number and other names of travellers on the PNR; Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight

shall be responsible for collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities and for exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with Europol. As condition for the information sharing, art. 9, para. 3, of PNR Directive establishes that the competent authorities of a Member State may directly request the PIU of any other Member State to provide them with PNR data that are kept in the latter's database only when necessary in cases of emergency and through a reasoned request. Data could also be transferred to a third country.

3. Migrants and travellers' data protection according to the current regulatory framework and its shortcomings

Arts. 7 and 8 of the EU Charter of Fundamental Rights safeguard the right to the respect of private life and the right to the protection of personal data respectively. Moreover, art. 16 TFEU states that everyone has the right to the protection of his personal data and establishes a legal basis for the adoption of rules relating to the processing of personal data by EU institutions, bodies, offices and agencies, and by the Member State when carrying out activities which fall within the scope of EU law[27].

The ECJ has played a relevant role in interpreting these articles, ensuring a very high level of protection of personal data in the light of the fundamental right to respect for private life in relation to legal acts adopted for security purposes. In the leading case *Digital Rights Ireland* [28], the Court provided a preliminary ruling concerning the validity of Directive 2006/24/EC on the retention of data related to electronic communications services or of public communications networks. In evaluating the conformity of the EU legal acts to the right to data protection, the European judges have assessed compliance with the principles of necessity and proportionality. Indeed, according to Art. 52(1) of the Charter, any limitation on the exercise of the rights and freedoms must be provided for by law, respect their essence and, subject to the

---

number, departure date, arrival date, departure port, arrival port, departure time and arrival time); All historical changes to the PNR listed in numbers 1 to 18.

[27] This article has fostered the previous art. 286 TCE that established the application to the Community institutions and bodies of the acts on the protection of individuals with regard to the processing of personal data. The adoption of the first Directive on the data protection of individuals was before the Lisbon Treaty, on the legal basis of the Art. 95 TCE. It is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, now repealed by Regulation 2016/679, cit. See, among others, B. CORTESE, *ART. 16 TFUE*, in A. Tizzano (a cura di), *Trattati dell'Unione Europea*, MILANO, 2014; ID., *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *DUE*, 2013, p. 313 ss.; F. DUMORTIER, *La protection des données dans l'espace européen de liberté, de sécurité et de justice*, in *Journal de droit européen*, 2010, p. 33 ss.

[28] In *Digital Rights Ireland* case, the ECJ has invalidated a directive that establishes the retention of data related the electronic communication for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism for the exceeding of the limits imposed by the principle of proportionality and necessity, Judgment of the ECJ of 8 April 2014, C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger*, ECLI:EU:C:2014:238. About the judgement see, among others, O. LYNSKEY, *The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital. Rights Ireland*, in *CMLR*, 2014, p.1789 ss; M.-P. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, in *ELR*, 2014, p.835 ss.; O. Pollicino, *Diritto all'oblio e conservazione di dati. La Corte di giustizia a piedi uniti: verso un digital right to privacy*, in *Giur. Cost.*, 2014, p. 2949 ss.

principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union. Moreover, the *proportionality test* requires that acts of the EU institutions must be appropriate for attaining the objectives they pursue must not exceed the limits of what is appropriate and necessary in order to achieve those objectives[29].

The Court has fleshed out the right to data protection and the test of necessity and proportionality in *Google Spain*[30] and in *Schrems*[31], although in these cases the Court was not called upon to balance the data protection right against an objective of general interest such as the fight against crime. That balancing exercise has re-emerged in the Court's opinion on the agreement between Canada and the EU on the transfer and processing of Passenger Name Record (PNR) data[32]. The Court has underlined that PNR data, taken as a whole, may reveal a complete travel itinerary, travel habits, relationships existing between air passengers and the financial situation of air passengers, their dietary habits or state of health, and may even provide sensitive information about those passengers. Following a thorough analysis on the justification for the interferences resulting from the envisaged agreement, the Court has stated that the agreement was incompatible with Articles 7, 8 and 21 and Article 52(1) of the Charter of Fundamental Rights of the European Union. This analysis was based *inter alia* on the respect for the essence of the fundamental rights here analysed, on the appropriateness of the processing of the PNR data having regard to the objective of ensuring public security, on the necessity of the interferences entailed by the envisaged agreement, and on the effective protection of the individual rights of air passengers (the right to information, the right of access and the right to correction and the right to redress). Then, the Judges have spelled out several conditions that the agreement must comply with in order to be compatible with the protection established by the Carter.

Therefore, the ECJ case-law[33] could be a parameter in the evaluation of the migrants and travellers' data protection according to the current regulatory framework.

Also noteworthy is the role of the European Data Protection Supervisor (hereinafter: EDPS) and of the ECJ in the enforcement of data protection. The EDPS is consulted by the European Commission when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. As we will see hereinafter, the EDPS has played its role by adopting opinions in which underlines the critical aspects of the legal proposal and suggests amendments.

We will see that the compliance evaluation of the regulatory framework on the data acquisition, the data retention and the information sharing related to the third-country citizens, travellers and migrants to the data protection right has to be accomplished considering two

---

29 See G. Caggiano, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Media Laws*, 2018, p. 64 ss., spec. p. 70.

30 ECJ, 13 May 2014, C-131/12, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, ECLI:EU:C:2014:317.

31 ECJ, 6 October 2015, C-362/14, *Schrems*, ECLI:EU:C:2015:650.

32 ECJ, 26 July 2017, Opinion 1/15, ECLI:EU:C:2017:592.

33 On the protection of personal data see, among others, G. MARTINICO, *Art.* 7, and O. POLLICINO, M. BASSINI, *Art.* 8, both in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea,* Milano, 2017. About the limits on interference with the right to the protection of personal data in the case law of the Court of Justice, see G. CAGGIANO, *L'interoperabilità fra le banche-dati dell'Unione sui cittadini degli Stati terzi*, in *Diritto, Immigrazione e Cittadinanza*, 2020, p. 169, spec. p. 172.

dimensions. On the one hand, the potential collection of a large amount of data and the risk of use for different purposes than those for which the data were collected, and, on the other hand, the protection of persons whose data are collected, for instance in the event of errors.

Recently, a new general Regulation on data protection[34] and a specific Directive[35] on data protection in the area of police and justice has improved the data protection legal framework, both applicable as of May 2018. Moreover, a new Regulation rules the protection of individuals with regard to the processing of personal data by EU institutions and bodies[36].

As explained above, the SIS Regulation allows the sharing of the alerts, therefore the sharing of the data, of TCN for a purpose that is much broader than the objective of the previous SIS, considering the new functionalities connected to investigative grounds. Moreover, the alert now includes biometric data and it should imply greater guarantees for TCN's data protection. In this context, the issuing of alerts related to a TCN that has been convicted in a Member State of an offence carrying a penalty involving deprivation of liberty of at least one year could be considered not proportionate[37]. This, even considering as cumulative the condition established by art. 24, para. 2, let. b), according to which shall be issued the alerts of TCN in respect of whom there are serious grounds for believing that he has committed a serious criminal offence or in respect of whom there are clear indications of an intention to commit such an offence in the territory of a Member State. It seems that there is no coherence between these two requisites: a serious criminal offence, usually, carries a penalty involving deprivation of liberty that is longer than at least one year.

Furthermore, we can underline that, unlike the legal acts that have established the other databases here considered, the SIS does not impose specific requirements as to the authorities that can have access to the alerts and the procedure. According to art. 44, paragraph 3, of SIS Regulation 2018/1862[38], beyond the authorities responsible for the border control or other police and customs checks, access "may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge, in the performance of their tasks, as provided for in national legislation, and by their coordinating authorities". The regulation does not limit access for availability of data for the prevention, detection and investigation of terrorist offences and other serious criminal offences, as established by VIS regulation[39], EES regulation[40] and

---

34 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, cit.

35 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, cit.

36 Regulation 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation 45/2001 and Decision 1247/2002/EC, OJ L 295.

37 See also art. 36 of the SIS II Decision, according to which an alert may be issued where there is clear indication that a person intends to commit or is committing a serious criminal offence, such as the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA.

38 The access to SIS by national competent authorities under SIS regulation 2018/1861, cit., is established by its art. 34.

39 See art. 3 of VIS Regulation, cit.

40 See art. 29 of EES Regulation, cit.

EURODAC regulation[41]. Moreover, no procedural requirement is established: art. 52 of SIS Regulation 2018/1862 only specifies that users may only access data which they require for the performance of their tasks[42]. This, despite regulations concerning the other database, where it is explicitly established that the designated authorities of the Member State may have access only in a specific case and following a reasoned written or electronic request[43].

SIS II seems unable to ensure an effective right to rectification[44], especially considering that identity fraud cases are not infrequent in this field. According to art. 57 of SIS Regulation 2018/1862[45], Member States can keep in its national files SIS data in connection with which action has been taken on its territory, and such data shall be kept in national files for a maximum period of three years The new regulation has limited the national use of SIS data establishing that a Member State shall not copy the alert data or additional data entered by another Member State from its N.SIS or from the CS-SIS into other national data files[46].

Moreover, it is important to underline that SIS Regulation establishes the mandatory cancellation of the data obtained without the respect of the necessity requirement and not the cancelation or the rectification of the national files in connection with which action has been taken on its territory, that can be retained for a maximum period of three years. This could mean that it is possible that a rectification made in the central system will not be followed automatically by a rectification in the national files. In any case of consultation by the national authority, a copy of the file containing incorrect information can be the prerequisite for subsequent actions also after the rectification or deletion in the central database. For this reason, in every case of deletion or rectification there should also be the introduction of a system of communication to all the authorities that have access to the incorrect information. This system of effective rectification of deletion shall be ruled in the EU regulation that establishes every information system, and not only by the general regulation on data protection or by the national rules[47].

On the other side, an N.SIS may contain a data file (a 'national copy') containing a complete or partial copy of the SIS database that can be shared with one or more Member States. In such a case, the Member State shall ensure, by means of the services provided by CS-SIS and by means of automatic updates, that the data stored in the national copy are identical to and consistent with the SIS database[48].

The ensure that the data stored in the national copy are identical to and consistent with the SIS database should be extended also to national files.

---

41 See art. 1, para. 2 and art. 6 Eurodac Regulation, cit.

42 About the processing of data see also art. 56 of Regulation 2018/1862, cit.

43 See art. 3 of Vis Regulation, cit., art. 31 of EES Regulation, cit., art. 19 of Eurodac Regulation, cit.

44 Rectification right is ruled by art. 59 and 67 of SIS Regulation 2018/1862, cit. See also art. 44 and 53 of SIS Regulation 2018/1861

45 See also Art. 42 of Reg. 2018/1861, cit.

46 See art. 56, par. 2, Regulation 2018/1862 and art. 41, par. 2, Regulation 2018/1831.

47 E. g. Art. 18 of Reg. 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, cited., and Art. 16 of 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, cited.

48 See Art. 4 and Art. 9, par. 2, of Reg. 2018/1861, cited, and the same articles of Reg. 2018/1862, cited.

The effective rectification and deletion right should be stressed also relating to the other databases. In this purpose, a step forward has been taken by EES Regulation, which states in its art. 43 that the competent authorities of the Member State shall cooperate actively to enforce the right of access to, rectification, completion and erasure of personal data[49].

The EES Regulation is also an example of the importance of the opinion given by the EDPS during the legislative procedure for the adoption of a legal act that can limit the right to the protection of personal data. In fact, it was established that the TNC has to provide his fingerprints for the rectification or deletion or for its identifying. In its Opinion, the EDPS highlighted that the prerequisite for a data subject to provide fingerprints when exercising his/her rights of access, correction and/or deletion of his/her personal data could have been an important obstacle to the effective exercise of these rights[50]. The EU co-legislators have agreed with this note and have established that "fingerprints may be requested […] only in duly justified cases and where there are substantive doubts as to the identity of the applicant. That information shall be used exclusively to enable that third-country national to exercise the rights referred to in paragraph 1 and shall be erased immediately afterwards"[51]. Nonetheless, the data retention periods of the EES data has been reduced from five to three years following the EDPS opinion[52].

The API and the PNR should be also examined with consideration to the right to data protection, even if they do not establish central databases. In these cases, we have a massive collection of travellers' data to allow the work of the intelligence, and arresting persons which are not suspects, before a crime is committed.

Such a system raises serious transparency and proportionality issues. According to the EDPS[53], the PNR scheme has been adopted without a comprehensive evaluation of the ability of the current existing instruments to reach the same purpose. So, "the non-targeted and bulk collection and processing of data of the PNR scheme amount to a measure of general surveillance"[54].

Some doubts about the compliance with the abovementioned principles live on after the adoption of the final text of the directive, which has not implemented the EDPS remarks. There is no specification about the criteria followed during the assessment of passengers to identify persons who require further examination[55]. The lack in the definition of the profiling standards could entail the noncompliance with the principles of transparency and of presumption of innocence[56]. The compliance of the API and PNR Directives with those principles should be assessed in the light of the Opinion of the Court on the EU-Canada Agreement PNR[57].

---

49 See art. 35, 52 and 53 of EES Regulation.

50 Opinion 6/2016 of the European Data Protection Supervisor Opinion on the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System, p. 3 e 17.

51 See Art. 52, para. 6, of EES Regulation, cited.

52 Opinion 6/2016, cit., p. 9.

53 Opinion 5/2015, Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

54 See p. 63.

55 See art. 6 of PNR Directive, cit.

56 It is important to underline that there is not any exemption about the data of the minors of at least 14 years, especially thinking that usually are not involved in terroristic crimes.

57 Opinion of 27 July 2017, cit.

4. Recent developments in the border management policy and in the safeguard of TCNs' data protection and some final considerations

EU border management policy has witnessed significant developments over the past years, due to the challenges posed by the influx of refugees and migrants, as well as the security concerns heightened by the terrorist attacks in Paris and Brussels.

The reform of the rules relating to border management through new smart systems had nevertheless several stops and go: the Commission submitted to the European Parliament and to the Council proposals relating to border management in 2008, 2011 and 2013 but some of the systems proposed faced criticisms from both co-legislators due to technical, operational and cost concerns, as well as important data protection concerns[58].

On 6 April 2016, the Commission released a second Smart Borders package[59], proposing the EES (in a revised version compared to the 2013 proposal) and the enrichment of the existing information systems as SIS II[60]. In the same year, the European Commission, in the context of the reform of the Common European Asylum System, has adopted a proposal for the amending of Eurodac[61].

Moreover, the European Commission has evaluated as inadequate the border controls of specific categories of travellers, such as third country nationals holding a long-term visa and the preventive control of third-country nationals who are exempt from holding a visa. For this purpose, the European Commission has adopted two proposals for a regulation to establish a framework for interoperability between EU information systems[62]. Therefore, according to the Regulation 2019/817 and the Regulation 2019/818, it has been established a framework for interoperability between EU information systems in the field of borders and visa and in the field of police and judicial cooperation[63].

---

58 See the Council Statement n. 5279/2016 of 18 January 2016.

59 Communication from the Commission to the European Parliament and the Council stronger and smarter information systems for borders and security, com/2016/0205 final.

60 See COM/2016/0882 final. The proposal has been followed by the adoption of Regulations 2018/1861 and 2018/1862, both cited.

61 Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM/2016/0272 final/.

62 Proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM(2017) 793 final; Proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM/2017/0794 final. See T. QUINTEL, *Interoperability of EU databases and access to personal data by national police authorities under Article 20 of the Commission proposals*, in *European data protection law review*, 2018, p. 470.

63 Regulation 2019/817 and Regulation 2019/818, both cited. About the interoperability see S. PEYROU-PISTOULEY, *L'interopérabilité des systèmes d'information au sein de l'Union européenne : l'efficacité au prix d'un fichage de masse*, in *Revue du droit de l'Union européenne,* 2019, p. 143.

In addition, a new centralised database has been established: the European Travel Information and Authorisation System (ETIAS),[64] which will gather information of visa-exempt third-country national; and the European Criminal Records Information System for third-country nationals (ECRIS-TCN)[65] that will share information on previous convictions against third-country nationals. The necessity of ECRIS is still debatable, especially considering the SIS II. It gives rise to the same doubts as to the protection of personal as those expressed with reference to ETIAS[66].

The interoperability will establish a connection between the existing information systems (SIS, VIS and Eurodac) and the new information systems (EES, ETIAS and ECRIS-TCN). The interoperability system will be managed by four new interoperability components that will allow to detect multiple identities and counter identity fraud: the European search portal (ESP); Shared biometric matching service (shared BMS); Common identity repository (CIR); Multiple-identity detector (MID). Interoperability between the EU information systems should allow those systems to supplement each other in order to facilitate the correct identification of persons.

Even if it is not possible to examine in depth the functioning of interoperability at this juncture, we would like to express some remarks about the usefulness and, at the same time, the obtrusiveness of the new central system in case of abuse: we have to consider that we are faced with the creation of a new centralised database that would contain information about millions of TCN, including their biometric data. For this reason, the personal data protection of the recorded individuals should be particularly strong.

On the one hand, the ESP will indicate whether data or links exist with other databases, but the system will only show each authority the data that it can already obtain under each regulation establishing the individual databases. BMS and CIR, on the other hand, constitute systems which, by linking data in various databases, can be considered new databases. This means that the data, originally acquired on the basis of a single database, with a specific function, can also be accessed in the context of other searches[67].

Furthermore, from a practical point of view, given the potential negative effects derived from incorrect information, an effective system of rectification should be implemented. Therefore, regarding the right of rectification and deletion, eu-LISA should be entrusted with a more active role.

As we can understand from art. 42, par. 3, of both the interoperability Regulations, eu-Lisa can authorize the copying of the data media. Moreover, each authorised authority, after

---

64 Regulation 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236.

65 Regulation 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation 2018/1726, OJ L 135.

66 See the Summary of the Opinion of the European Data Protection Supervisor on the Proposal for a European Travel Information and Authorisation System (ETIAS), OJ 2017, C 162.

67 See G. CAGGIANO, *L'interoperabilità fra le banche-dati dell'Unione sui cittadini degli Stati terzi*, *cit.*, p. 180, who specifies that it is difficult to argue that the conditions of access to the data and the purposes for which it was collected remain unchanged compared to the original instruments of the individual databases, because what could not be obtained before from the individual databases can highlight a person's history and characteristics.

having received information from a consultation, will at least use it to continue its specific activity[68].

In any case, there is the possibility that off-line copies of personal data can be the basis for judicial inquiry or other legal consequences. Also in this case, it is fundamental to guarantee an effective rectification or erasure of the personal data that are wrong or unlawfully issued.

Of course, Member States are responsible for the rectification or deletion request, considering that they insert the data in the databases and they are potentially nearest to the individual. Nonetheless, considering that eu-LISA will keep logs of all data processing operations by national authorities[69], the European agency is in the best position to control the effective updating of the information used by the national authorities and to inform the authorities which have requested the information that the update has taken place. For this purpose, this task shall be included among the responsibilities of eu-LISA.

Considering the impact that such a system has on the right to the protection of personal data and the potential effect that incorrect information may have on an individual's life, the EDPS's opinion, arguably, should have been followed more closely. The European legislator, in turn, should lay down a more consistent, coherent and comprehensive legal framework where EU databases for border management and for law enforcement embed a set of core data protection principles such as: purpose limitation, state-of-the-art security protocols, proportionate data retention periods, data quality, data protection by design, traceability, effective supervision, and dissuasive sanctions for misuse[70].

---

68 It cannot be excluded, in fact, that the information acquired may also be used for further activities.

69 See, between the others, art. 10, 16 and 24 of the Interoperability proposal, cited.

70 This set of core data protection principles has been defined by the EDPS Giovanni Buttarelli, see EDPS Opinion 7/2017 on the new legal basis of the Schengen Information System, para. 6. About the content of the data protection principles, in addition to the above mentioned articles, see P. DE HERT, C. RIEHLE, *Data protection in the area of freedom, security and justice. A short introduction and many questions left unanswered*, in *ERA Forum*, 2010, p. 159 ss.; D. ALONSO BLAS, *Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom*, in *ERA Forum*, 2010, p. 233 ss.