Revista de Derecho Político

Monográfico con motivo del XL aniversario de la Constitución Española de 1978 (II)

UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

UNED

MADRID enero-abril 2018 N.º 101

SOME FURTHER REFLECTIONS ON THE DIRECTIVE (EU) 2016/681 ON PNR DATA IN THE LIGHT OF THE CJEU OPINION 1/15 OF 26 JULY 2017

SUSANNA VILLANI

TABLE OF CONTENTS

© UNED. *Revista de Derecho Político*
N.º 101, enero-abril 2018, págs 899-928

Fecha recepción: 16.05.2017
Fecha aceptación: 9.01.2018

SOME FURTHER REFLECTIONS ON THE DIRECTIVE (EU) 2016/681 ON PNR DATA IN THE LIGHT OF THE CJEU OPINION 1/15 OF 26 JULY 2017

SUSANNA VILLANI[1]

Investigadora predoctoral.
Universidad Nacional de Educación a Distancia, UNED (España),
Università di Bologna (Italia),

1. INTRODUCTION

Over the last decades the EU and other Western countries have been witnesses of an increase of serious and organised crime, such as trafficking in human beings and drugs, as well as of terrorist attacks thereby triggering them to collaborate among themselves in order to strengthen the measures aimed at fighting against crime and terrorism. Among the others, the exchange of information between public authorities in order to prevent severe criminal acts has become one of the more pressing points to be discussed and regulated at international level. And, among the information that national enforcement authorities could consider relevant for combating criminals and terrorists, and that, therefore, should be covered by specific rules on data protection, there are also the Passenger Name Record (PNR) data collected by air carriers for their own commercial purposes[2]. In fact, PNR data contain several different types of information provided by passengers during the reservation and booking of tickets and that are then necessary for air carriers to manage flight reservations and check-in sys-

[1] Alma Mater Studiorum – Università di Bologna, via Zamboni 33 – 40126 Bologna. Email: susanna.villani2@unibo.it

[2] See, Communication from the Commission to the Council and the Parliament – Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, COM(2003) 826 final. For further insights, see NINO M. (2010), "The protection of personal data in the fight against terrorism. New perspectives of PNR European Union Instruments in the Light of the Treaty of Lisbon", *Utrecht Law Review*, Vol. 6, 2010, pp. 62-85; NUNZI A. (2007), "Exchange of Information and Intelligence Among Law Enforcement Authorities: A European Union Perspective", *Revue Internationale de Droit Penal*, Vol. 78, pp. 143-151.

tems. These records comprise a number of details concerning travel dates, travel itinerary, ticket information, telephone numbers, personal contact details, credit card numbers, the travel agent at which the flight was booked, seat number and baggage information, as well as other information of ethnic or religious character such as the choice of the meal[3]. So, over the years, collecting and analysing PNR data have become crucial activities by which police authorities can identify dangerous passengers and take appropriate measures in order to prevent, detect, investigate and prosecute terrorism and other serious crimes. First of all, they can be used for a pre-arrival and pre-departure assessment of passengers according to a pre-emptive strategy. Secondly, in comparison to other kinds of collected information that can be used just to verify the identity of known suspects, PNR data can be necessary for identifying suspects hitherto "unknown" before their arrival or departure thus preventing the commitment of a crime. Finally, their use can be relevant in the phase of investigation, prosecution and unravelling of criminal networks after a crime has been committed.

The use of this kind of information has always inspired concerns in relation to the respect of fundamental rights, particularly that to privacy and data protection. In this regard, it is worth to recall the multiple warnings on the lack of transparency, safeguards and controls from States on digital privacy launched by the UN High Commissioner[4] for Human Rights as well as by major NGOs[5] operating in this field. Indeed, in the absence of a clear and comprehensive international legal framework regulating this new area, there is a concrete risk that national legislations are not capable to adequately protect privacy rights over increasing security reasons. And, with reference to data protection, at European regional level it is worth to recall the positions assumed by the European Court of Human Rights (ECtHR) which have been based on a number of legal instruments adopted by the Council of Europe. In effect, the ECtHR has had an extraordinary role in urging States to guarantee major protection of personal data by especially dealing with the surveillance[6] and interception of communications[7] as well

[3] PNR data should not be confused with Advance Passenger Information (API), comprising biographical data resulting from passports thus being more limited in scope than PNR data. Moreover, the use of API is regulated by a specific act, that is the API Directive, which provides that API data should be made available to border control authorities for improving border controls and combating irregular immigration. See, Council Directive 2004/82/EC of 29 August 2004 on the obligation of carriers to communicate passenger data, *OJ L 261*, 6.8.2004.

[4] The High Commissioner for Human Rights of the United Nations has expressed its concerns in its Report, *The right to privacy in the digital age*, 30 June 2014, UN Doc. A/HRC/27/37.

[5] See, *OHCHR Consultation in connection with General Assembly Resolution 68/167 "The Right to Privacy in the Digital Age*", 1 April 2014.

[6] *See, European Court of Human Rights, Klass and others v. Federal Republic of Germany, Application no. 5029/71, Judgement of 6 September 1978; Uzun v. Germany, Application no. 35623/05, Judgement of 2 September 2010.*

[7] See, European Court of Human Rights, *Malone v. United Kingdom*, Application no. 8691/79, Judgement of 2 August 1984; *Copland v. United Kingdom*, Application no. 62617/00, Judgement of 3 April 2007.

as the data storage by public authorities[8]. Indeed, as underlined several times by the ECtHR, the systematic collection and storage of personal information fall within the scope of the right to a private life enshrined in Article 8 ECHR and, therefore, a balance between the need of data-collecting by public authorities on the one hand and the protection of individual interests and rights on the other one has to be reached. For this purpose, the ECtHR has developed a set of criteria that must be respected and that include: the duty to inform the person concerned in advance with regard to the storage of his or her information, evident limitations on the power to store and use the information collected, a clear definition of the categories of individuals against whom surveillance measures can be taken and of what kind of information to be recorded and for what purpose[9].

The instruments adopted by the Council of Europe and the jurisprudence of the ECtHR partially overlap those of the European Union mainly in terms of common principles[10] progressively consolidated within the EU legal order by the jurisprudence of the European Court of Justice (CJEU) which has fuelled the need to establish a common approach across the EU as for the use of PNR data in the respect of fundamental rights[11]. Indeed, as recently stressed by the CJEU in *Tele2* and *Watson*[12], "while the effectiveness of the fight against serious crime, in particu-

[8] See, European Court of Human Rights, *S. and Marper v. United Kingdom*, Applications no. 30562/04 and 30566/04, Judgement of 4 December 2008; *Leander v. Sweden*, Application no. 9248/81, Judgement of 26 March 1987.

[9] See, European Court of Human Rights, *Segerstedt-Wiberg and Others v. Sweden*, Application no. 62332, Judgement of 6 June 2006. For further details on the ECtHR jurisprudence on data protection, see Brower E. (2009), "The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?" , *CEPS Working Document* , No. 320.

[10] Among these qualitative requirements it is appropriate to recall: the respect of legality, proportionality, purpose limitation and data security; safeguards for the processing of sensitive data; specific set of rights including the right to access, modification and correction of data; allocation of powers of control over national and European supervisory authorities; assessment of the level of protection in third countries in case of data processing.

[11] For deeper insights on the expansion of the right to data protection in the EU legal order, see, Vermeulen M., Bellanova R. (2012), "European 'smart' surveillance: what's at stake for data protection, privacy and non-discrimination?", *Security and Human Rights*, No. 4, pp. 119-133; Granger M., Irion K. (2014), "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", *European Law Review*, Vol. 36, pp. 835-850; Fabbrini F. (2015), "Human rights in the digital age: the European Court of Justice ruling in the Data Retention Case and its lessons for privacy and surveillance in the United States", *Harvard Human Rights Journal*, Vol. 28, pp. 65-95; Brkan M. (2016), "The Unstoppable Expansion of the EU Fundamental Right to Data Protection Little Shop of Horrors?", *Maastricht Journal of European and Comparative Law*, Vol. 23, pp. 812-841;

[12] See, CJEU, Judgment of 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele 2 and Watson et al.*, ECLI:EU:C:2016:970. For some insights on this case, see Woods L., "Data Retention and National Law: the ECJ Ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)", *EU Law Analysis*, available at www.eulawanalysis.blogspot.it.

lar organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight"[13].

The use of these data by EU Member States' law enforcement bodies is nothing new[14], but the national measures sensibly diverge in several aspects, including the purpose of the system, the period of data retention, the structure of the system, the geographic scope, the modalities of transport covered as well as the level of protection of personal data and information. Seen the great potential of collecting PNR data, the Commission has proposed more than once the establishment of a EU-wide PNR scheme which harmonised national provisions in this field. For this purpose, mainly after the entry into force of the Lisbon Treaty, the EU institutions have acted on two different levels: on the one hand, a number of instruments and mechanisms operating at internal level have been approved to increase the collaboration among Member States, and, on the other hand, there have been attempts to conclude international agreements with the most concerned States.

At internal level, after multiple failures, in 2011, the Commission submitted a proposal of Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes which, however, received some criticism with reference, *inter alia*, to its necessity and to the respect of the principle of proportionality. The project regained attention after the terrorist attacks of January 2015 in Paris, when counter-terrorism issues reached the top of the political agenda, both in the Member States most concerned and at EU level. On 21 April 2016 the Council adopted Directive (EU) 2016/681 in order to regulate the transfer of PNR data from the airlines to the Member States, as well as the processing of these information by the competent authorities.

As for the conclusion of bilateral agreements on PNR data transfer in the context of the fight against serious transnational crime and terrorism, the first-ever international agreement for the transfer of personal data was negotiated with the United States in 2004, but was annulled by the EU Court of Justice in 2006, because of the lack of "an appropriate legal basis"[15]. On May 2010, the

[13] See, CJEU, *Tele 2 and Watson et al.*, *cit.*, para. 103.

[14] Within the EU France, Denmark, Belgium, Sweden and the Netherlands have enacted relevant legislation and have tested using PNR data. Also the United Kingdom has its own PNR system.

[15] *See, CJEU, Judgment of 3 May 2006, Joined Cases C-317/04 and C-318/04, European Parliament v. Council of the European Union and Commission of the European Communities, ECLI:EU:C:2006:346. For comments on this judgment, see* MENDEZ M. *(2007), "Passenger Name Record Agreement – European Court of Justice: Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US Grand Chamber Judgment of 30 May 2006, Joined cases C-317/04 and C-318/04, European Parliament v. Council and Commission", European Constitutional Law Review, Vol. 3, pp. 127-147.*

European Parliament adopted a Resolution on the launch of negotiations for PNR data agreements with third countries by calling for a coherent approach on the use personal information for law enforcement and security purposes, establishing a single set of principles to serve as a basis for the new agreements[16]. To that end, the Commission issued three proposals aimed at authorising the initiation of negotiations with the United States, Australia and Canada and in 2012 two agreements were signed and concluded with the United States[17] and Australia[18], with the approval of the Parliament. Instead, the bilateral agreement on the processing and transfer of PNR data by air carriers to the Canadian competent authorities was signed in 2014, but the European Parliament, whose consent is necessary for the conclusion of the agreement, requested an opinion from the CJEU under Article 218(11) TFEU as to whether the agreement satisfied fundamental human rights standards and whether the appropriate Treaty base had been used for the agreement. On 26th July 2017, the CJEU has declared that the envisaged EU-Canada agreement is incompatible with EU law in its current form[19].

Against this complex and multifaceted background, which intertwines the internal and external dimensions, the present contribution is aimed at providing some further reflections on the actual attempts to balance the need to guarantee security and the protection of personal information and privacy rights in the field of the fight against crime. To this end, after a brief reconstruction of the path towards major cooperation in information exchange between Member States, it will be illustrated the content of the Directive 2016/681 by reproposing its main points of light and shadow with reference to the protection of fundamental rights as conceived within the EU legal order. Moreover, in a wider horizon of analysis, it will be provided for a comment on the recent CJEU opinion on the PNR Agreement between the EU and Canada in order to assess the potential future challenges to be faced both by the PNR Directive and by other international agreements.

[16] *See, Passenger Name Record (PNR) European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, OJ C 81E, 15.3.2011, p. 70.*

[17] See, Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, *OJ L 215*, 11.08.2012, p.5.

[18] See, Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, *OJ L 186*, 14 July 2012, p. 4.

[19] See, CJEU, Opinion 1/15 on the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 26 July 2017, ECLI:EU:C:2016:656.

2. HISTORICAL AND LEGAL BACKGROUND: ASSESSING THE NECESSITY OF AN ACT ON PROCESSING PNR DATA AT EU LEVEL

Member States have always preferred to fight against crime in an autonomous way according to the traditional logic of State sovereignty in guaranteeing national security. But, the terrorist attacks in the United States in 2001, as well as the bombings in Madrid and London in 2004 and 2005, combined with the absence of internal border controls under the Schengen Convention, has made evident that terrorism may have a transnational character[20]. This awareness has triggered dynamic process towards more cooperative policies in response to the threats posed by serious crimes and terrorism within the EU territory[21]. Since the European Commission and the specialised EU law enforcement agencies do not have autonomous investigative capabilities and are not in charge of operational law enforcement activities to effectively prevent and combat cross-border serious crimes and terrorism, practical cooperation between the police and customs authorities of EU Member States is, indeed, essential. Undoubtedly, one of the main challenges for the EU and its Member States has been the improvement of updated information exchange between criminal intelligence units in a timely and accurate manner for successfully preventing, detecting and investigating criminal conduct. As matter of the fact, sharing available information such as personal data has been foreseen in a number of multilateral conventions, but always according to a certain degree of discretion from Member States.

One of the first examples of sharing personal data as a specific aspect of effective cooperation between European law enforcement authorities is the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985[22], which has established the Schengen Information System. Processing personal data of specific categories of persons and making those available by using one central information system for different authorities in the States that implemented the Schengen Convention was seen as a necessary compensatory measure for creating a high level of security in an area of free movement of persons. Another step in improving cooperation between law enforcement authorities was marked by the Europol Convention[23]

[20] See, HEUPEL M. (2007), "Adapting to Transnational Terrorism: The UN Security Council's Evolving Approach to Terrorism", *Security Dialogue*, Vol. 38, pp. 477-499.

[21] For further details see, BROUWER E., CATZ P., GUILD E., (2003), *Immigration, Asylum and Terrorism: A Changing Dynamic in European Law*, Nijmegen, Recht & Samenleving; CARRERA S. (2005), "What Does Free Movement Mean in Theory and Practice in an Enlarged EU?", *European Law Journal*, Vol.11, pp. 699-721.

[22] See, The *Schengen acquis* – Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *OJ L 239*, 22.9.2000.

[23] *See, Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), OJ C 316, 27.11.95.*

and Eurojust Decision[24], which established two European offices with the specific task to facilitate the exchange of law enforcement information. Although these forms of cooperation express the genuine intention to share information for security reasons, they do not establish specific obligation to do so or overcome the main problem for the law enforcement agencies, that is the need for a formal request and, sometimes, judicial authorisation.

In 2005 the European Council realised its blueprint (the so-called "Hague Programme"[25]) in the area of freedom, security and justice by inviting the EU institutions to improve the effectiveness and interoperability of the existing EU information systems, such as the Visa Information System (VIS)[26] and the "second generation" Schengen Information System (SIS II)[27]. Therefore, it was set an innovative approach to the cross-border exchange of law enforcement information by introducing the principle of "availability", which has become operational since 1 January 2008. This means that throughout the Union, all information available to national law enforce-

[24] See, Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, 2002/187/JHA, *OJ L 63*, 6.3.2002 and Council Decision on the strengthening of Eurojust and amending Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, 5347/3/09 REV 3, ANNEX, 15.07.2009.

[25] See, The Hague Programme: strengthening freedom, security and justice in the European Union, *OJ C 53*, 3.3.2005, and the Council and Commission action plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union, *OJ C 198*, 12.8.2005.

[26] The Visa Information System (VIS) consists in a central information technology system and in a communication infrastructure that links this central system to the national ones. In particular, VIS connects consulates in non-EU countries and all external border crossing points of Schengen States by processing data and decisions relating to applications for short-stay visas to visit or to transit through the Schengen Area. The system can perform biometric matching and scan fingerprints thus allowing for faster, more accurate and more secure checks. See, Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), 2004/512/EC, *OJ L 213*, 15.6.2004.

[27] The Schengen Information System (SIS II) enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons. The alert does not only contain information about a particular person, but also clear instructions on what to do when the person has been found. The SIS was upgraded in early 2015 to facilitate and accelerate information exchange on terrorist suspects and to reinforce the efforts of Member States to invalidate the travel documents of persons suspected of wanting to join terrorist groups outside the EU. The scope of the SIS II is defined in three legal instruments, that are Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *OJ L 381*, 28.12.2006 and Commission Decision 2008/333/EC of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II), *OJ L 123*, 08.05.2008. For further details, see European Commission, *Overview of information management in the area of freedom, security and justice*, COM(2010)385 final, 20.07.2010, pp. 5-6, available at http://www.eapmigrationpanel.org/files/research/en/SIS_II_paper_liberty_security_formatted1-1.pdf. See, BROUWER E. (2008), *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System Leiden*, Leiden, Martinus Nijhoff Publishers.

ment authorities should also be made accessible to law enforcement authorities in other Member States through reciprocal access to and interoperability of national databases, or direct access, including for Europol, to existing central EU databases such as the SIS[28]. The idea was thus to make fully available and pool real-time records acquired at national level regardless of their cross-border nature by linking common databases. In this perspective, the principle of availability seems approaching to the methodological principle of mutual recognition which supports the whole field of judicial cooperation in criminal matters and that presumes the need for ensuring mutual trust and confidentiality between national police and security authorities as for the sharing of highly sensitive information concerning their own nationals[29]. In sum, the principle of availability marks a fundamental shift from traditional forms of information exchange between national agencies organised upon bilateral or multilateral agreements and formal requests procedures[30].

Following the Hague strategy, the Commission presented its proposal for a Council Framework Decision on the exchange of information under the principle of availability[31]. The motion extended the scope of application of the principle to a wide range of data fields by laying down, *inter alia*, a clear obligation for the Member States to collect, store and give access to certain types of information available to their authorities also to other Member States (Recital 6). But, notwithstanding the incentive of the European Council, the potentially far-reaching—but doubtful in terms of data protection—implications of the draft Framework Decision were not fully endorsed by the Council that, instead, adopted in 2006 the so-called "Swedish Framework Decision"[32]. This strategy was based on a more limited policy principle, that is that of "equivalent access", according to which the conditions applicable to cross-border data exchange should be no stricter than those regulating domestic access. From an operational point of view, it simplified the exchange of information as national contact points were requested to handle urgent requests for information and to respond to requests for information and intelligence in a short timeframe. But, in comparison to the target of the Hague Programme, neither an obligation on Member States to provide information nor a direct information exchange between authorities have been set in the new strategy, thus being welcomed by supporters of data protection.

---

[28] See, The Hague Programme, *cit.*, point 2.1.

[29] See, Fletcher M. (2008), *EU Criminal Law and Justice, Elgar European Law,* pp. 94-97.

[30] *For further insights on the principle of availability, see* Gutiérrez Zarza A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe, Springer; Jones C. (2011), Implementing the principle of availability: the European Criminal Records Index Systems, The Information Exchange Platform for Law Enforcement Authorities, Statewatch Analysis.*

[31] See, Council Framework Decision on the exchange of information under the principle of availability, COM (2005) 490, 12.10.2005.

[32] See, Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union ("Swedish Framework Decision"), *OJ L 386*, 29.12.2006.

In the same year, the Council and the European Parliament adopted the Data Retention Directive, then declared invalid by the EU Court of Justice in the *Digital Rights Ireland*[33], to enable national authorities to combat serious crime by retaining telecommunication traffic and location data[34]. Furthermore, in 2008, the Council approved the so-called "Prüm Decision"[35] which implemented, within the EU legal framework, most of the provisions contained in the intergovernmental Prüm Treaty concluded by some EU Member States in 2005[36]. The purpose of the extra-EU tool, and thus of the Council Decision, was to establish more effective mechanisms for cross-border police cooperation and the exchange of DNA profiles, fingerprints and vehicle registration data. Despite the powers to transmit such data to end-users are governed just by national law, the Prüm Decision introduced a new element in law enforcement cooperation, that is the obligation upon Member States to make the mentioned data available—by means of the Trans European Services for Telematics between Administrations (TESTA II) communications network—in order to facili-

[33] See, CJEU, Judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238. In this regard, see BIGNAMI F. (2007), "Privacy and Law Enforcement in the European Union: The Data Retention Directive", *Chicago Journal of International Law*, pp. 233-255; FEILER L. (2010), "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", *European Journal of Law and Technology*, Vol. 1, pp. 1-34; GUILD E., CARRERA S. (2014), "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", *CEPS Paper in Liberty and Security in Europe*, available at www.ceps.eu; KONSTADINIDES T. (2014), *Mass Surveillance and Data Protection in EU Law: The Data Retention Directive Saga, in European Police and Criminal Law Co-Operation. Swedish Studies in European Law*, Oxford, Oxford University Press.

[34] See, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ L 105/24*, 15.03.2006. For details on this act, see JONES C., HAYES B. , *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, SECILE —Securing Europe through Counter-Terrorism—Impact, Legitimacy & Effectiveness, available at http://www.statewatch.org/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf (accessed on 26 April 2017); NI LOIDEAIN N. (2010), "The EC Data Retention Directive: legal implications for privacy and data protection", in AKRIVOPOULOU C., PSYGKAS A. (eds.), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, IGI Global, p. 256 ff.

[35] See, Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, *OJ L 210*, 6.8.2008.

[36] The Treaty of Prüm was signed on 27 May 2005 in Germany by seven Member States (Belgium, Germany, France, Luxembourg, the Netherlands, Austria and Spain) and entered into force in 2006. Eight additional Member States (Finland, Italy, Portugal, Slovenia, Sweden, Romania, Bulgaria and Greece) has then formally declared their intention to accede to it in order to further develop cooperation in combating terrorism, cross-border crime and illegal immigration. For an evaluation of this Treaty, see, European Parliament – Committee on Civil Liberties, Justice and Home Affairs, *Working document on a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime*, Rapporteur: Fausto Correia, 10 April 2007.

tate the prevention and prosecution of crimes[37]. Therefore, the existing more or less voluntary exchange of information in these areas was attempted to be replaced by an obligation to provide information and also to create for certain categories of personal data an infrastructure enabling other law enforcement authorities to have access to available data. However, Member States' implementation of the Prüm Decision encountered many technical and administrative difficulties and the majority has failed to do so[38].

Such a brief overview makes evident that, despite there was a wide consensus that effective prevention requires more information, the pre-Lisbon intergovernmental arrangements and procedures—not involving the European Parliament—applicable to EU police and criminal law measures has made it more difficult the adoption of common positions over these issues. In addition, it cannot be ignored that the panoply of legal instruments adopted was scarcely coherent and, on the other side, poorly respectful for fundamental rights.

The entry into force of the Lisbon Treaty has partly changed the general approach to this topic, by reinforcing the supranational dimension of safeguarding against and preventing threats to public security. Indeed, it has included judicial and police cooperation in criminal matters among shared competences between the Union and Member States as part of the broader cooperation in the Area of Freedom, Security and Justice[39]. In particular, Article 82 TFEU—which regulates judicial cooperation in criminal matters—now requires the European Parliament and the Council to adopt, by means of ordinary legislative procedure, measures aimed at, *inter alia*, facilitating cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions. Furthermore, as for police cooperation, the new provisions enshrined in the Treaties prescribe the involvement of all the Member States' competent authorities, including police, customs and other specialised law enforcement services for the prevention, detection and investigation of criminal offences (Article 87 TFEU). To this end, it has been allowed the adoption, under ordinary legislative procedure, of acts providing for harmonising measures related to, among the others, the collection, storage, processing, analysis and exchange of relevant information[40].

---

[37] See, Council Decision 2008/615/JHA, *cit.*, Article 5.

[38] **See,** BELLANOVA R. (2008), "The "Prüm Process": The Way forward for EU Police Cooperation and Data Exchange", in GUILD E., GEYER F.(eds.), *Security Versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate Publishing, pp. 203-221; JONES C. (2012), "Complex, technologically fraught and expensive. The problematic implementation of the Prüm Decision", *Statewatch Journal*, Vol. 22.

[39] For deeper insights on the innovations brought by the Lisbon Treaty in this area, see DOUGAN M. (2008), "The Treaty of Lisbon 2007: winning minds, not hearts", *Common Market Law Review*, Vol. 48, pp. 617-703.

[40] See, Article 87(2)(a) TFEU.

As a result, in the wake of the Stockholm Programme[41] the Commission tried to launch the idea of a new EU legislative framework on PNR data[42]. Gained the support both of the European Parliament and the Council, the Commission thus issued on 2 February 2011 a specific proposal for a Directive on the use of Passenger Name Record data[43]. However, this proposal encountered serious criticism from many quarters—from the European Data Protection Supervisor[44] to the Working Party on Data Protection[45] —in relation to its necessity and proportionality as well as for its impact on citizens' rights. Indeed, besides strengthening the requirement of major cooperation among Member States in the field of judicial and police activities, the Lisbon Treaty has also reinforced the provisions concerning individual rights by attributing to the EU Charter of fundamental rights the same legal value of the treaties and, more specifically, by expressly acknowledging the right to data protection in Article 16 TFEU. As a result, the first draft was rejected by the European Parliament's LIBE Committee[46] and on April 2013 the adoption of an instrument concerning the collection and processing of PNR data was no longer considered as a priority.

3. THE DIRECTIVE 2016/681 ON PNR DATA: A CRITICAL ANALYSIS

The project regained attention in 2015 when the European Union started witnessing major terrorist attacks and the recruitment of EU citizens for fighting with the self-proclaimed Islamic State in their own countries in Europe[47]. By considering

[41] See, The Stockholm Programme – An open and secure Europe serving and protecting citizens, *OJ C 115*, 4.5.2010.

[42] See, Communication of the European Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM/2010/0492 final, 21.9.2010.

[43] See, 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, COM(2011) 32 final, 2.2.2011.

[44] See, Opinion of the European Data Protection Supervisor 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, 25 March 2011.

[45] See, Opinion 10/2011 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, 5 April 2011.

[46] See, Report 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 (COM(2011)0032—C7-0039/2011—2011/0023(COD)) , Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Timothy Kirkhope, 29 April 2013.

[47] See, European Parliament resolution of 11 February 2015 on anti-terrorism measures, 2015/2530(RSP), point 13.

the number of citizens from France, Germany, the United Kingdom and Belgium who have used air travel as part of their journey to conflict zones in the Middle East to join the terrorist groups, there have been calls for the EU to introduce more efficient instruments for monitoring passenger airline travels out of and to EU Member States[48].

In the aftermath of the terrorist attacks in Paris in November 2015, the LIBE Committee gave the green light for the conclusion of the first provisional deal between the Parliament and the Council on 2 December 2015. The plenary of the European Parliament adopted its position[49] on 14 April 2016 by requesting the Council to approve immediately the PNR Directive. The Council adopted unanimously the Directive on 25 April 2016 and the final text was signed on 27 April 2016 by the President of the Parliament and by the Dutch Minister of Defence on behalf of the Council[50].

Directive (EU) 2016/681 on the collection and processing of European Passenger Name Records (PNR) for preventing, detecting, investigating and persecuting terrorist actions and serious crimes, requires Member States to introduce provisions laying down obligations on air carriers operating international flights between the EU and third countries to forward PNR data of all passengers to the Passenger Information Unit (PIU) established at domestic level for this purpose (Article 4). Furthermore, according to Article 2 of the Directive, Member States are given the discretion to extend the regime set out in the Directive to intra-EU flights, or to a selection of them. Seen the recent terrorist attacks provoked by European citizens or long-term residents in their own States or in neighbour Member States, it is unsurprising that all participating Member States have then declared their intention to make use of their discretion to collect also data belonging to persons moving around the EU territory.

Once received, the data should be stored and analysed by the national competent authorities referred to in Article 7 in order to "identify persons who were previously unsuspected of involvement in terrorism or serious crime" (Recital 7) prior their

[48] See, Tzanou M. (2015), "The War against terror and transatlantic information sharing: spillovers of privacy or spillovers of security?", *Utrecht Journal of International and European Law*, Vol. 31, pp. 87-103.

[49] See, 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 – Outcome of the European Parliament's first reading, 15 April 2016.

[50] See, Directive 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*, 4.5.2016. According to Article 18, Member States have two years for transposing the Directive by adopting laws, regulations and administrative provisions necessary to comply with it. For some insights on the content of Directive 2016/681 see, *ex multis*, Birzu B. (2016), "Prevention, Detection, Investigation and Prosecution of Terrorist Offenses and Other Serious Crimes by Using Passenger Name Record (PNR) Data. Critical Opinions. De Lege Ferenda Proposals", *Perspectives of Business Law Journal*, Vol. 195, pp. 195-206.

arrival in or departure from the Member State; as well as to further update or create new criteria for evaluating any person's involvement in terrorist offences or in the crimes listed in Annex II of the Directive. As for the period of retention and depersonalisation, Article 12 sets that data can be retained in the PIUs for a period of time not exceeding five years, after which the data should be deleted; and that the data should be depersonalised through masking out of specific elements after a period of six months.

Finally, according to Article 9 Member States shall ensure that, when necessary, all the relevant information are exchanged among each other and delivered also to Europol through relevant information exchange networks and electronic means. The above mentioned provisions thus may contribute to the development and establishment of a permanent EU PNR system focusing on the common fight against the limited knowledge about those who could be involved in terrorism or other serious crimes.

3.1. Security and data protection: towards a balance?

In comparison to the previous draft proposals, Directive 2016/681 now seems to contain more robust safeguards to ensure full compliance with the proportionality principle and guarantee a high level of fundamental rights protection in comparison to the original proposal which gained a lot of criticism.

First of all, important references to data protection have been made not only within the whole text of the Directive: it has been also included a specific provision (Article 13), which asks for the respect of the principle of non-discrimination in ensuring "protection of personal data, rights of access, rectification, erasure and restriction and rights to compensation and judicial redress". As for the transmission of PNR data by air carriers to the PIUs it has been chosen the so-called "push method" meaning that the Member States do not have direct access to the carriers' IT systems, but they have to request the air carriers to transfer the required PNR data to the authority. In comparison to the "pull method" which is based on an uncontrolled copying of PNR data from the air carriers' reservation system, the chosen method seems to offer a higher level of data protection.

Furthermore, since any passenger's personal data can indiscriminately be collected and checked by national authorities, in order to ensure that the processing of data of innocent and unsuspected persons remains as limited as possible, it has been explicitly prescribed that the list of PNR data obtained by the PIUs should not be based on race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation[51]. And, in the event that PNR data revealing such information are received by the PIUs, they shall be

[51] See, Directive 2016/681, *cit.*, Article 6(4).

deleted immediately. These are, indeed, highly sensitive information whose disclosure would not be acceptable.

The Directive also provides that a decision taken by competent authorities that produces an adverse legal effect on a person should not be taken following the automated processing of PNR data: the transfer of any personal information—even to third countries—shall be made only in a *case-by-case* basis and in a non-automated way[52].

Apart from prescribing specific dispositions and mechanisms for data protection, in line with the suggestions of the European Data Protection Supervisor[53], the Directive now specifies the features of the authorities that would have access to PNR data and requires Member States to ensure that an independent national supervisory authority is responsible for advising and monitoring how PNR data are processed[54]. In fact, Article 5 introduces the data protection officer in the PIU as independent figure responsible for monitoring and implementing all the relevant safeguards during the processing of personal data. In addition, for the sake of transparency, Member States are required to list the national competent authorities entitled to request and receive PNR data for the prevention, detection, investigation or prosecution of terrorist offences or serious crime to be notified to the Commission and published in the Official Journal of the European Union. Last but not least, Article 15 creates a direct link with the Framework Decision 2008/977/JHA, now Directive 2016/680, by entrusting the national supervisory authority also with the responsibility for advising on and monitoring the application of the provisions illustrated within the national territory, as well as dealing with complaints lodged by any data subject and verifying the lawfulness of the data processing. In this regard, also the Commission keeps a special task, as Article 19 of the PNR Directive requires it to conduct by 25 May 2020 a review of the Directive with particular attention to the compliance with the applicable standards of protection of personal data, the necessity and proportionality of collecting and processing PNR data, the length of the data retention period, and the effectiveness of exchange of information between the Member States.

Finally, it should be noted that the Directive—although it stresses the need to strengthen effective cooperation between national authorities and includes the opportunity to designate a single PIU for two or more Member States—does not mention the principle of availability. The choice to not introduce the concept of free flow of information between national authorities as proposed by the Hague Programme does

[52] See, Directive 2016/681on the use of passenger name record (PNR) data, *cit.*, Article 6(6).

[53] See, European Data Protection Supervisor, 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, 24 September 2015.

[54] See, Directive 2016/681, *cit.*, Article 15.

not lie just on the fact that prescribing uncontrolled processing and sharing of personal information could jeopardise national prerogatives and responsibilities in guaranteeing security within their borders[55], but also on the necessity to ensure full data protection. Indeed, notwithstanding the principle of availability can be justified by the fact that the abolishment of internal borders calls for exchange of police information and combination of forces between the Member States, an indiscriminate sharing of sensitive data may bring to a misuse that hardly could be detected and subjected to remedy. This may be the reason why Article 9(2) of the Directive establishes that the transmission of PNR data not yet depersonalised—and thus still comprising very sensitive information such as address or general personal remarks—can be done just in case of duly substantiated reasons or of emergency. Moreover, in the event that the requested data have been depersonalised through masking out of data elements, the PIU is able to provide the full PNR data (just) where it is reasonably believed its necessity for preventing, detecting, investigating and persecuting terrorist actions and serious crimes, and only when authorised to do so by a competent national authority.

It actually seems that the very Directive embodies instruments and safeguards that—albeit there is certainly room for improvement—not only respond to the needs of protection of fundamental rights, but also to the general necessity to assure coherence among policies and objectives in the field of data protection and judicial and police cooperation. However, as already stressed by some authors, the challenges that the system illustrated might pose to the protection of privacy and data protection rights are still acute[56].

3.2. The remaining long shadows over the right to privacy and data protection

Despite the mentioned positive elements of improvement, it cannot be neglected that some crucial shortcomings concerning data protection still affect the EU legal act now in force. And, one of the main reasons why concerns prevail is that, although PNR data can be used for a number of purposes encompassing surveil-

[55] *It should not be neglected that, despite the Lisbon Treaty abolished the pillar structure and included judicial and police cooperation in criminal matters among shared competences between the Union and Member States, according to Article 4(2) TEU and Article 72 TFEU national security still remains anchored to the responsibilities of Member States that jealously guard it.*

[56] See, Vavoula N. (2016), *"I travel, therefore I am a suspect: an overview over the EU PNR Directive", EU Immigration and Asylum Law and Policy Blog, available at http://eumigrationlawblog.eu/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/.* See, *ex multis*, Lowe D. (2016), «The European Union's Passenger Name Record Data Directive. 2016/681: Is It Fit for Purpose?», *International Criminal Law Review,* Vol. 16, pp. 856-884; Di Matteo F. (2017), «La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR?», *Diritti umani e diritto internazionale*, Vol. 1, pp. 213-235.

lance of criminals' movements and immediate reaction to a criminal conducts, the focus of the Directive is clearly oriented towards the prevention phase. As reported in the previous paragraphs, before the adoption of such a Directive the EU legal framework concerning storage and exchange of information covered just alleged and identified terrorists and criminals in order to facilitate their prosecution. In order to detect and persecuting persons potentially involved in criminal or terroristic affairs, the Directive now allows the systematic, blanket and indiscriminate transfer, storage and further processing of a wide range of personal data of millions of travellers from and to the EU. Such a prior and general assessment of all passengers on the basis of predetermined criteria decided by the respective PIUs and of special databases created at international level may clearly affect fundamental individual rights.

The system established by the PNR Directive could, indeed, lead to a strong interference with and impact on some fundamental rights and freedoms that the Lisbon Treaty has contributed to reinforce[57]. Before the entry into force of the Lisbon Treaty, legislation concerning data protection in the Area of Freedom, Security and Justice was divided between the first pillar in relation to private and commercial purposes, and the third pillar as for law enforcement purposes. The removal of the pillar structure and the acknowledgement of an independent individual right to data protection within a unique provision of primary law has provided a stronger legal basis for the development of a clearer and more effective data protection system that involves also the European Parliament. Moreover, the general scope of the provision makes it applicable also to the processing in the area of police and judicial cooperation. In this regard, it cannot be neglected that Declaration 21 attached to the Lisbon Treaty acknowledged that in the fields of judicial cooperation in criminal matters and police cooperation specific actions for the protection of personal data are necessary by virtue of their special nature[58].

The extreme relevance of Article 16 TFEU is, moreover, reflected by the coincidence of its content with that of Article 8 of the EU Charter of Fundamental Rights which has been integrated in the Lisbon Treaty. The drafters have thus deemed appropriate to provide for a independent legal basis for the establishment of an adequate legal package which responded to the necessity to guarantee full application to the provision of the EU Charter. Such a quasi-constitutional dimension of the right to data protection has an important consequence that is to further limit the margin

[57] See, Scirocco A. (2009), "Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?", *Common Market Law Review*, Vol. 46, pp. 1485-1525.

[58] See, Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation: "The Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields".

of appreciation of the States while reinforcing the test of proportionality when verifying the validity of a measure[59].

By contrary, according to the Directive 2016/681, on the basis of the data collected, law enforcement authorities are able to compile a rather complete profile of travellers' private lives, without, apparently, any limit. In this case, the collection and storage of personal information could thus bring to undermine the right to privacy (Article 7 of the EU Charter) that is naturally linked to data protection. Furthermore, a five-year data retention period could lead to discriminatory profiling of individuals. Therefore, at first sight, it could appear that, in the balancing between security needs and the protection of those fundamental rights enshrined in Articles 7 and 8 of the EU Charter as well as in Article 16 TFEU, the former prevail over the latter in a disproportionate way.

In addition, it is striking that the Directive is almost silent about the procedure of analysis of the collected data: it regulates the ways data can be taken and managed, but it does not indicate the criteria for performing the profiling procedure which clearly relies on the identification of behavioural patterns according to a probabilistic logic. This lack of clarity joins the concerns relating to the fact that the PNR Directive does not mention the so-called EU data protection package comprising the Data Protection Regulation[60] and the Directive for data protection in the police and justice sectors[61] which have been adopted in parallel by the European Parliament and the Council on 27 April 2016[62].

The storage and control of personal data movement could affect, however, not only the mere protection of individual privacy, but also the respect of the principle of presumption of innocence, since each traveller could be suspected even when there is no evidence capable of suggesting that its conduct is linked with a criminal offence.

---

[59] *See,* Blasi Casagran C. *(2016), Global Data Protection in the Field of Law Enforcement: An EU Perspective, Routledge Research in EU Law.*

[60] See, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *OJ L 119*, 4.5.2016.

[61] *See, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016. For comments, see* Akintunde Salami E. *(2017), The Impact of Directive (EU) 2016/680 on 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 on the Existing Privacy Regime, available at https://ssrn.com/abstract=2912449.*

[62] For an assessment on this issue, see Kuner C. (2014), "The European Union and the Search for an International Data Protection Framework", *Groening Journal of International Law*, Vol. 2, pp. 55-71; Di Francesco Maesa C. (2016), "Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)", *Eurojus.it* .

The operation of the PNR scheme, hence, contributes to reverse the presumption of innocence, whereby everyone can be a potential security risk, thus necessitating a specific assessment in order to confirm or disprove this presumption. According to some authors "we are dealing with a *mass surveillance tool* that (inevitably) reverses the presumption of innocence against passengers: each one is presumed a criminal suspect unless his or her profile hints at the opposite" (emphasis added)[63].

Even before, the procedure of processing appears to lack of transparency since the individuals concerned cannot be aware neither that public authorities gather and make use of their personal information, nor that they could be suspected of criminal misconducts. After the *Kadi saga*[64], which started with a claimant who had not been informed of the grounds for his inclusion in the list of individuals and entities subject to sanctions and that brought the CJEU to underline that the protection of fundamental rights forms part of the very foundations of the Union legal order, it is almost certain that the EU's PNR Directive will come next for review before the CJEU even if the process of implementation by the Member States is already underway. In this case, the potential task of the very Court in ruling on the consistency of the PNR Directive with the fundamental rights illustrated could not be effortless. After all, there is to say that at EU level those institutions aimed at promoting the EU citizens' rights and the proper application of EU law have never refrained from issuing their firm opinions with regard to the respect of the fundamental rights to data protection and privacy.

4. THE CJEU OPINION 1/15 ON THE EU-CANADA AGREEMENT: WHAT LEGAL CHALLENGES FOR THE PNR DIRECTIVE?

All the considerations and concerns proposed in the previous paragraph acquire even more relevance with reference to the agreements on data sharing concluded by the Union with third countries where the level of protection may considerably differ from that existing within the EU Members. The intention to conclude such agreements clearly reveals that the need to define a general and wide approach of cooperation on data transfer among States for fighting against terrorism is increasing. However, it cannot be underestimated the urgency repeatedly stressed at EU level to agree on the adoption of norms which ensure an equivalent level of protection of fundamental rights thereby pursuing a sort of internationalisation of the EU protection standards. As a result, as set both in *Digital Rights Ireland* and in

[63] See, De Hert P., Papakonstantinou V. (2015), "Repeating the Mistakes of the Past will do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling", *New Journal of European Criminal Law*, Vol. 2, pp. 160-166.

[64] For a comment on thistopic, see Gianelli A. (2013), "Exit Kadi", *Rivista di diritto internazionale,* Vol. 96, pp. 1244-1249.

Schrems[65], which has invalidated the Safe Harbour agreement between the US and the EU[66], any rule which includes the transfer of personal data to third countries must ensure the effectiveness of the control by national authorities for verifying the respect of an adequate level of data protection under EU law[67]. The processing of personal data to third countries cannot therefore diminish the degree of protection guaranteed at EU level.

In this regard, it is illustrative the tortuous path for the conclusion of the EU-US Privacy Shield replacing the mentioned Safe Harbour agreement and containing much more safeguards than the previous agreement. Indeed, on the basis of the requirements set out by the CJEU in the *Schrems* ruling, the Commission has worked on a new framework for transatlantic exchanges of personal data which provided a level of data protection that was "essentially equivalent" to that of EU law[68]. In April 2016, the Article 29 Working Party then supported by the European Parliament's resolution[69], whilst welcoming the efforts made, expressed concerns and outlined practical recommendations to improve the Commission's adequacy decision[70]. The Privacy Shield[71] was finally approved on July 2016 and boosted further by an international agreement[72] and a related Council Decision

[65] See, CJEU, Judgment of 6 October 2015, Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650.

[66] The CJEU invalidated the Harbour Decision exactly in the *Schrems* case, by concluding that the European Commission did not state in its Safe Harbour decision that the US ensures an adequate level of protection and that the decision was accordingly invalid, without there being any need for it to examine the substance of the Safe Harbour principles (*Schrems* case, paras. 97-98). For deeper comments, see, Nino M. (2015), "La Corte di giustizia UE dichiara l'invalidità del sistema di Safe Harbour: la sentenza Schrems", *Quaderni di SIDIBlog*, Vol. 2, pp. 286-293; Carrera S., Guild E. (2015), "The End of Safe Harbor: What Future for EU-US Data Transfers?", *Maastricht Journal of European and Comparative Law*, Vol. 22, pp.651-655; Rossi dal Pozzo F. (2016), "La tutela dei dati personali tra esigenze di sicurezza nazionale,interessi economici e diritti fondamentali della persona (dal *Safe Harbour* al *Privacy Shield*)", *Rivista di diritto internazionale*, Vol. 99, pp. 690-724; Giattini A. (2016), "La tutela dei dati personali davanti alla Corte di giustizia dell'UE: il caso *Schrems* e l'invalidità del sistema di 'approdo sicuro'", *Diritti umani e diritto internazionale*, Vol. 1, pp. 247-255.

[67] See, Kuner C. (2017), "Reality and Illusion in EU Data Transfer Regulation Post *Schrems*", *German Law Journal*, Vol. 18, pp. 883-918.

[68] In particular, the Commission assured that the new agreement contained strong obligations on companies, safeguards and transparency obligations on US government access to EU citizens' data, redress mechanisms (including an Ombudsman) and a monitoring system.

[69] See, European Parliament resolution of 26 May 2016 on transatlantic data flows (2016/2727(RSP)).

[70] See, Article 29 Working Party Opinion 01/2016 of 13 April 2016 on the EU-US Privacy Shield draft adequacy decision.

[71] See, Commission Implementing Decision 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, *OJ L 207/1*, 12.07.2016.

[72] See, Agreement between EU and US on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses, 2017, *OJ L 336/3*.

concerning data exchanges between law enforcement authorities (the so-called "Umbrella Agreement")[73]. Some weeks later, however, the Article 29 Working Party issued a statement on the revised privacy shield by expressing a number of remaining concerns on both commercial aspects (e.g. a lack of specific rules on the right to object, the complexity of the redress system), and on US public authorities' access to data (e.g., the lack of stricter guarantees on the independence and power of the Ombudsperson, based so far only on written assurances)[74]. In a similar vein, on April 2017 the European Parliament adopted a new resolution on the adequacy of the protection afforded by the EU-US agreement[75] that the Commission will have to take into account on occasion of the joint annual review scheduled for September 2017. It is thus evident that, albeit all the improvements made, the Privacy Shield could be brought in front of national and European courts by individuals, European data protection authorities or by privacy advocacy associations, with regard to its adequacy and the level of protection of fundamental rights. As matter of the fact, a recourse against the Privacy Shield adequacy decision has been already filed by Digital Rights Ireland against the European Commission on 16 September 2016[76].

As set out in the 2015 European Agenda on Security, the Union's future approach to the exchange of PNR data with non-EU countries will depend, in particular, on the Opinion by the Court of Justice of the European Union on the envisaged EU PNR Agreement with Canada[77]. Accordingly, in order to complete the framework on the attempts of balancing between security and data protection as well as on the future legal challenges the PNR Directive will have to face, the following sections will briefly address the opinion issued by the CJEU with reference to the EU-Canada agreement on the transfer of PNR data and its potential impact on the whole PNR dossier.

4.1. The CJEU's Opinion 1/15 on the Agreement between the Union and Canada on PNR data processing

The agreement between the EU and Canada sets that PNR data collected from passengers for reserving flights between Canada and the Union are transferred to the

[73] See, Council Decision 2016/2220 of 2 December 2016 on the Conclusion, on Behalf of the European Union, of the Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, *OJ L 336/1*, 02.12.2016.

[74] See, Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, 26 July 2016.

[75] See, European Parliament resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield (2016/3018(RSP)).

[76] See, General Court, Case T-670/16, *Digital Rights Ireland v. Commission*, 16 September 2016 .

[77] *See, European Commission Communication to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, Brussels, COM(2017) 7 final, 10.1.2017, section 4.*

Canadian competent authorities and then processed and used in order to prevent and detect terrorist attacks and other serious transnational criminal offences. In particular, it provides for a data storage period of five years and lays down requirements in relation to PNR data security and integrity, immediate masking of sensitive data, rights of access to and correction and erasure of data, and for the possibility of administrative and judicial redress.

The proposal issued by the Commission on 19 July 2013, was adopted by the Council which sought the Parliament's approval of the draft decision relating to the conclusion of the agreement. But, on 25 November 2014, in application of Article 218(11) TFEU the very Parliament decided to request the Court to provide its opinion concerning the compatibility of the agreement with Article 16 TFEU and with Articles 7, 8 and Article 52(1)) of the EU Charter. The doubts of the European Parliament originated, firstly, from the opinion issued by the European Data Protection Supervisor (EDPS) on 30 September 2013[78]. In that opinion, which the Council did not take into consideration for amending the initial proposal of agreement to be signed, the EDPS had raised a number of questions concerning the necessity and proportionality of the PNR schemes and of mass transfers of PNR data to third countries, as well as the lack of adequate data protection safeguards. These concerns have been, therefore, assessed both by the Advocate General and by the very Court which has recently expressed its firm position on that by issuing the first-ever opinion on the compatibility of a draft international agreement with the EU Charter of Fundamental Rights.

On 26 July 2017, a few months after the Advocate General's opinion[79], the European Court of Justice disclosed its position by concluding that the PNR agreement could not be approved in its current form because several of its provisions are incompatible with the fundamental rights recognised by the EU. As a general point, the Court has adopted a detailed level of review of the PNR agreement by following Advocate General Mengozzi in extending its rulings in cases such as *Schrems*, *Digital Rights Ireland* as well as *Tele2/Watson* to international agreements. Indeed, by premising that the proposed agreement has two different but inextricably linked objectives—safeguarding public security and safeguarding personal data—, it observed that, even though the driver for the need to PNR data was protection of public security, the transfer of data would be lawful only if data protection rules were

[78] See, Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, available at https://edps.europa.eu/sites/edp/files/publication/13-09-30_canada_en.pdf .

[79] See, Opinion 1/15 of the Advocate General Paolo Mengozzi delivered on 8 September 2016, ECLI:EU:C:2016:656. For a comment on the Opinion 1/15, see Lassalle M. (2016), *Opinion 1/15: AG Mengozzi looking for a new balance in data protection*, available at http://europeanlawblog.eu/2016/10/18/opinion-115-ag-mengozzi-looking-for-a-new-balance-in-data-protection-part-ii/.

respected[80]. In fact, as stressed in Opinion 1/15, "the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental right enshrined in Article 7 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference"[81]. Consequently, even though interferences with these rights may be justified, they have to respect the very essence of those rights and freedoms which are intended to be limited and, furthermore, such limitations must be necessary and genuinely meet objectives of general interest recognised by the Union.

The Court thus found that PNR data might reveal considerable details about an individual, such as their travel habits, relationships, and financial situation, as well as sensitive information. Thus, the Court acknowledged that the systematic transfer and storage of PNR data to Canada and the rules foreseen in the Draft Agreement would entail an interference with the fundamental rights to respect for private life under Article 7[82] and to the protection of personal data under Article 8 of the Charter[83]. However, by departing from the AG position as well as its own conclusions in *Tele2/Watson*, the Court has pulled back a bit from the prohibition against "general and indiscriminate retention" of data and has found that interference with the fundamental rights to privacy and data protection may be justified[84]. In any event, to avoid the risk of any abuse, the legislation should set down "clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards"[85], specifically indicating in what circumstances and under which conditions a measure providing for the processing of such data may be adopted especially when automated processing is involved. But, in the envisaged agreement, with particular reference to sensitive data, this clarity and other solid justifications beyond the general one of public security and prevention of terrorism are lacking[86]. In particular, following verification of passenger data and permission to enter Canadian territory, the Court expected that the use of that data during the passengers' stay in Canada should be based on new justifying circumstances having objective nature and

[80] See, CJEU, Opinion 1/15, *cit.*, para. 94.

[81] See, CJEU, Opinion 1/15, *cit.*, para.124.

[82] See, CJEU, Opinion 1/15, *cit.*, para.125.

[83] See, CJEU, Opinion 1/15, *cit.*, para.126.

[84] See, CJEU, Opinion 1/15, *cit.*, para. 151. For a comment on this, see KUNER C. (2017), "Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15", *VerfBlog*, available at http://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/.

[85] See, CJEU, Opinion 1/15, *cit.*, para. 141.

[86] See, CJEU, Opinion 1/15, *cit.*, para. 165.

that this should be subject to prior review by an independent body[87]. Furthermore, the Court found that the continued storage of the PNR data of all air passengers after their departure from Canada which the envisaged agreement permits goes beyond what is strictly necessary[88].

With regard to the disclosure of PNR data to government authorities, the Court reiterated the standards stated in *Schrems* and, in particular, that data transfers to third countries require a level of protection that is "essentially equivalent" to that under EU law[89]. However, the proposed agreement does not seem to meet the same level of protection as that guaranteed by EU law. The Court found that, when there is no risk of jeopardising the investigations, individuals must have a right to have their data rectified and be notified individually when their data are used by a judicial authority or independent administrative body[90]. Moreover, as for to automated analyses of PNR data, because of the margin of error, any positive result should be subject to "individual re-examination by non-automated means" before any measure adversely affecting a passenger is taken[91]. Finally, the Court held that the Draft Agreement does not sufficiently guarantee that oversight of compliance with its rules is carried out by an independent authority within the meaning of Article 8(3) of the Charter [92]. Accordingly, by taking up the package on the Privacy Shield with the United States, the Court went on to require a more structured approach which envisaged either an international agreement between the EU and a third country, or an adequacy decision of the Commission[93].

4.2. Some reflections on the impact of Opinion 1/15 on the PNR dossier

Opinion 1/15 sets out for the first time the conditions under which international agreements may be used to legalize international data transfers. The CJEU Opinion contain a lot of issues of interest that could be discussed from a range of perspectives, but for the purposes of the present contribution, this section will do justice mainly to the interplay between the Opinion and the illustrated Directive 2016/618. In fact, in the light of the long and highly contested history of the PNR Directive, there are many actors who are impatient to revise the measure.

In effect, Opinion 1/15 provides for some veiled criticism towards Directive 2016/681 that could represent a good starting point of a future recourse before the Court of Justice. The first element concerns the individual right to be notified of the

[87] See, CJEU, Opinion 1/15, *cit.*, paras. 201-203.
[88] See, CJEU, Opinion 1/15, *cit.*, para. 209.
[89] See, CJEU, Opinion 1/15, *cit.*, paras. 134 and 214.
[90] See, CJEU, Opinion 1/15, *cit.*, paras. 223-224.
[91] See, CJEU, Opinion 1/15, *cit.*, para. 173.
[92] See, CJEU, Opinion 1/15, *cit.*, para. 231.
[93] See, CJEU, Opinion 1/15, *cit.*, para. 214.

transfer of personal data. Indeed, in its Opinion, the CJEU clearly denounces the fact that the agreement merely lays down a rule regarding transparency requiring the Canadian Competent Authority to make available on its website certain information of a general nature relating to the transfer of PNR data and its use, without establishing any obligation to notify air passengers individually specific criteria defining the profiling procedure[94]. As already recalled in the previous section, also the PNR Directive does not include any reference to the individual right to be notified thus inspiring doubts on the level of protection of the right to information. The conclusions reached by the Court could hence represent an important point of challenge for the Directive at stake. By remaining in the sphere of individual rights, it is instead quite weird the lack of any comment by the Court to the issue of the systemic transfer of large quantities of data, that could bring to mass surveillance and ultimately to undermine the principle of presumption of innocence. In this aspect, that would be quite interesting also for the validity of Directive 2016/681, Opinion 1/15 does not appear as strong and emphatic as in *Tele2/Watson* and, therefore, just an eventual ruling on the very Directive will be able to clarify such a point.

In a broader perspective, it is remarkable the objection made by the Court on the lack of any distinction between data collected on all passengers that travel to, and stay in, Canada, and the retention and use of data after passengers have left the territory of Canada. Even though this element may appear secondary for the PNR Directive because Opinion 1/15 concerns an agreement between the Union and a third country and, therefore, major safeguards have to be included, it actually could have serious repercussions on the EU Directive. Indeed, not even the PNR Directive makes such a distinction, but only foresees masking/depersonalization procedures of collected PNR data after six months from until maximum retention period of five years. Besides, it makes no reference to the fact whether a person stays in the EU's territory or not. As a result, one could imagine that under Directive 2016/681 the retention and use of PNR data is possible also when the individual has left the country of travel thereby going beyond what is strictly necessary to prevent acts of terrorism or other crimes. There is to say that, whether the EU intends to establish a wide regime providing for adequate safeguards and oversight mechanisms, the EU laws in all these fields should overlap in order to guarantee effective protection to the EU citizens.

As matter of the fact, in comparison to the outcome of the AG's opinion, the conclusions provided by the CJEU does not seem just to negatively affect the PNR Directive, but to some extent also to positively support it. In the first place, it has to be stressed that the Court has judged PNR data collection and analysis for the purposes of the prevention and investigation of serious crimes and terrorism as proportionate and justifiable because strictly necessary to the final aim. Moreover, it has to be underlined the different positions assumed by the AG and by the Court with

[94] See, CJEU, Opinion 1/15, *cit.*, para. 220.

reference to the five-year period retention of data that characterises also the PNR Directive which, moreover, does not distinguishes between categories of data. Indeed, while the AG had challenged it by concluding that it exceeds what is necessary, the Court found that interference with the fundamental rights to privacy and data protection may, under the right circumstances, be justified by a general objective of the EU even though this involves a data retention period of five years. Furthermore, it is significant that the Court explicitly referred to the PNR Directive as a model to limit the potential for discrimination or collection of especially sensitive data under PNR data exchanges as well as to perform the data analyses not through automated but human interventions[95].

At the end of the day, since the functioning of the EU PNR and the EU-Canada schemes are similar, the answer of the Court might have a significant far-reaching impact on the validity of the PNR Decision, but also on the planned international PNR agreements with other States. In this regard, it is quite interesting that, looking at the procedural issues, the Court has found that the correct legal basis for draft agreement were Article 16(2) TFEU and Article 87(2)(a) TFEU, but not Article 82(1)(d) TFEU. This could spell trouble for other PNR agreements of the EU that rely on Article 82(1)(d) TFEU as a legal basis, such as those with Australia and the United States. Moreover, even though the EU-US Privacy Shield now enshrines a number of safeguards of transparency and redress mechanism, the CJEU Opinion could represent a risk also for this agreement which, as argued by the Article 29 Working Party in July 2016, does not provides for strict guarantees of independence of the supervisory authority that, instead, has been considered essential by the Court in its reasoning. Finally, it seems that many international agreements concluded by the Union—including the future one with the United Kingdom—could potentially be open to challenge in light of the strict standards the Court has applied with reference to data protection for complying with the EU Charter. Time will tell what impact this opinion will have on the progress of those talks.

5. FINAL REMARKS

Member States have always been dominated by certain reluctance to pool and coordinate national forces or, even more, entrusting the European Union with a stronger coordination capacity. Moreover, whilst national authorities are well-disposed to deploy their instruments and resources for responding to serious crimes, they demonstrate major scepticism in the preventive phase where a high level of mutual trust and confidentiality between national police and security authorities is required as for the sharing of highly sensitive information. But, in the aftermath of the attack on the Twin Towers and under the increase in serious criminal offences in many parts

[95] See, CJEU, Opinion 1/15, *cit.*, para. 166.

of the world, enhanced cooperation in cross-border data exchange between law enforcement authorities has been sought in order to prevent and respond to these threats having, often, transnational character and involving international travel. In a context of tension between right to security and right to privacy, between collective and individual rights, the major challenge is, therefore, to balance in a proportionate way both the interests in order to have a secure area of freedom and security and at the same time respect for fundamental rights.

Against this background, the PNR Directive may represent a useful instrument for assessing passengers on international flights from and to the Member States and, ultimately, for combating terrorism. However, it is understandable the emergence of concerns over potential illegitimate restrictions of individuals' right to privacy and data protection, that are fully recognised both by the ECHR and the EU Charter. In particular, it remains questionable the lack of transparency in the phase of data processing which makes the individuals concerned unaware that public authorities gather and make use of their personal information, or that they could be suspected of criminal misconducts. But, on the other hand, it cannot be underestimated the fact that the PNR Directive contains some substantive and procedural safeguards which—in formal terms—contributes to re-balance potential violations of fundamental rights. In addition, even though the legal nature of this act—which leaves to the Member States the task to implement it—could potentially bring to 27 different systems, the adoption of a common legislation at EU level has overcome the tendency to develop diverging national PNR systems as manifestation of the statehood logic in dealing with security matters and has sensibly reduced the risk of infringement of data protection rules. Furthermore, there is no doubt that the whole process—made of Commission Communications, resolutions of the European Parliament and opinions on the respect of the right to data protection—represents the very core of European democracy. Until a single overarching EU information system having multiple purposes and much more independence is created, the PNR Directive can be thus seen as another piece of the jigsaw in the elaboration of an Area of Freedom, Security and Justice aimed at realising an even more secure EU for its citizens. The simultaneous adoption of the PNR Directive and the package on data protection makes then ear the intention to embark on a shared regulatory process capable of taking into account needs of protection against external (and internal) threats and against potential violations of fundamental rights.

In any case, given the conclusions reached by the CJEU in Opinion 1/15, it is not excluded a request from the European Parliament to the EU Court of a judgement on the compatibility between some provisions of the PNR Directive and the rules of primary law on data protection. Moreover, it will trigger major legal debates on data transfers to third countries: next steps may include initiatives aimed at indicating alternative data transfer mechanisms so as to increase legal certainty over how personal data should be transferred from the EU. However, it cannot be neglected the risk that some third countries become more hesitant to invest time and resources to

© UNED. *Revista de Derecho Político*
N.º 101, enero-abril 2018, págs 899-928

conclude an international agreement on data protection with the EU, knowing that it might later be revised by the CJEU. The ultimate effects of the judgment will be hence seen in the coming years when the EU will try to negotiate further agreements on data protection and data sharing with third countries and international organisations.

Título:

Nuevas reflexiones sobre la Directiva (UE) 2016/618 a la vista de la Opinión 1/15 del Tribunal de Justicia de 26 de Julio 2017

Sumario:

Abstract:

Over the last decades, it has arisen the need for increased cooperation between law enforcement authorities in making more systematic use of the data furnished by those moving to and from the States in order to prevent, detect, investigate and prosecute terrorism and other serious crimes. On 21 April 2016 the Council adopted Directive 2016/681 in order to regulate PNR data transfer from the airlines to the Member States, as well as the processing of this data by the competent authorities. Its validity, with particular reference to the balance between needs of security and the respect of fundamental rights, such as the right to respect for private life and the right to the protection of personal data, could be challenged after the conclusions reached by the CJEU in its Opinion on the EU-Canada agreement on PNR transfer.

Resumen:

En la última década, ha surgido la necesidad de una mayor cooperación entre las autoridades nacionales de los diferentes Estados para hacer un uso más sistemático de los datos entre ellos para luchar contra el terrorismo y otros crímenes. El 21 de abril de 2016, el Consejo adoptó la Directiva 2016/681 para regular la transferencia de los datos PNR de las líneas aéreas a los Estados miembros, así como el tratamiento de estos datos por

las autoridades competentes. Su validez, en relación con el equilibrio entre las necesidades de seguridad y el respeto de los derechos fundamentales, como el derecho al respeto de la vida privada y el derecho a la protección de los datos personales, podría ser impugnada como consecuencia de la opinión emitida por el TJUE sobre el acuerdo UE-Canadá en relación a la transferencia de datos personales.

Key words:

Fight against terrorism – information exchange – PNR data – air carriers – data protection – right to privacy – international agreement

Palabras clave:

Lucha contra el terrorismo – intercambio de información – PNR data – compañías aéreas – protección de datos – derecho de privacidad – acuerdos internacionales