Utrecht Law Review published by igitur

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

Michele Nino*

1. Introduction

International terrorism has a transnational character.[1] As a consequence, the cooperation, the coordination, and the exchange of information between law enforcement authorities of the EU Member States, their agencies, Europol, and judicial authorities constitute fundamental elements in order to guarantee the effectiveness of the fight against terrorism and organized crime.[2]

In the context of the fight against international terrorism, after 11 September 2001, the European Union concluded Agreements with third States, such as the United States, Canada and Australia, aimed at transferring and processing air passengers' personal data and is currently preparing a European system for regulating the retention, transmission and treatment of such data.[3]

Collecting and processing personal data involves two categories of data: PNR data (Passenger Name Records) and API data (Advance Passenger Information). The former, which contains a large and diverse quantity of data, concerns the data collected and extracted from various travel documents (usually air flights), and, in general, it can include data contained in passports, telephone numbers, travel carriers, credit card numbers, seat numbers and other elements.[4] Even before 2001, air carriers collected and kept such data but only for commercial purposes, so these activities did not have investigative purposes and were not aimed at combating

* Ph.D., Researcher in International Law, Faculty of Law, University of Salerno (Italy). Lawyer at the Naples Bar (Italy). Professional address: University of Salerno, Faculty of Law, Department of International Studies, Via Ponte don Melillo 1, 84048 Fisciano (SA), Italy; email: mnino@unisa.it

1 M. Heupel, 'Adapting to Transnational Terrorism: The UN Security Council's Evolving Approach to Terrorism', 2007 *Security Dialogue* 38, no. 4, pp. 477-499.

2 See Exchange of information between the law enforcement authorities of the Member States, available online at <http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/l14151_en.htm>; Communication from the Commission to the Council and the European Parliament of 16 June 2004: Towards enhancing access to information by law enforcement agencies, COM(2004) 429; 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; EU Terrorism Situation and Trend Report 2007, available online at <http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/TESAT2007.pdf>, p. 36; see also A. Nunzi, 'Exchange of Information and Intelligence Among Law Enforcement Authorities: A European Union Perspective', 2007 *Revue Internationale de Droit Penal* 78, no. 1/2, pp. 143-151; R. Bellanova, 'The "Prüm Process": The Way forward for EU Police Cooperation and Data Exchange', in: E. Guild *et al.* (eds.), *Security Versus Justice?: Police and Judicial Cooperation in the European Union*, 2008, pp. 203-221.

3 See Sections 4-6, *infra*.

4 See Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, WP 66, 24 October 2002, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp66_en.pdf>, p. 3.

international terrorism and organised crime. Over the years, collecting and analysing PNR data have become important activities by which police authorities can identify dangerous passengers and take appropriate measures. API data, which consists of official data resulting from passports, contains data concerning passengers that is more limited than PNR data, because it includes the name, the nationality, the passport number, the date of birth and other details concerning passengers on flights. In the European Union, the collection of API data is provided for by Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.[5]

The aims of this article are: 1. to identify the normative and structural deficiencies of the EU legal system by which the right to personal data protection is not adequately protected, especially in the context of the activities falling in the second and third pillars of the European Union, such as anti-terrorism activities; 2. to analyze in a detailed manner the dispositions of the above-mentioned PNR tools by examining their negative effects on the right to privacy of individuals in the European Union; 3. to provide innovative and coherent solutions in order that PNR instruments will, in the future, become important and legal tools in the fight against international terrorism, taking into account the positive changes that the Treaty of Lisbon will produce concerning the European Union's institutional system and structure, and, as a consequence, concerning the protection of the right to personal data protection and EU counter-terrorism measures. The Agreement will affect the new choices of the European Union regarding the fight against terrorism and the processing and transfer of PNR data.

As analyzed in the present article, the current structure of the European Union, which is founded on three pillars, is not as such to ensure an adequate and comprehensive protection of the right to personal data protection.[6] First of all, the article addresses international and Community norms regarding those rights.[7] After having examined the scope of the so-called Convention No. 108 adopted by the Council of Europe, which is the first European regional instrument in this area, the analysis shifts to an examination of Directive 95/46, which is the principal Community norm regarding the right to privacy.[8] The scope of application of this Directive is excluded as far as activities falling into the second and third pillars (which involve crucial areas, such as public security, public defence and state security) are concerned. The reduced scope of Directive 95/46 and the pyramidal structure of the European Union have created a legislative lacuna in the EU legal system by which the fundamental rights and freedoms of individuals, such as the right to personal data protection, have been seriously prejudiced. This also occurred in the context of the anti-terrorism measures. In this regard, the article also examines Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed within the framework of police and judicial cooperation in criminal matters.[9] This decision, that forms part of the third pillar, is an important legal tool, but it is not able to adequately protect personal data.

Thereafter, the article addresses the improvements that the Treaty of Lisbon will produce concerning the institutional organization of the European Union, the protection of the right to privacy, and the counter-terrorism activities.[10] In this context, the article examines in a detailed manner the norms provided by the EU-USA PNR Agreement, the EU-Canada API/PNR Agree-

5 Directive 2004/82/EC, *OJ* L 261, 6.8.2004, p. 24.
6 See Section 2.3, *infra*.
7 See Sections 2.1- 2.3, *infra*.
8 See Section 2.2, *infra*.
9 See Section 2.3, *infra*.
10 See Section 3, *infra*.

ment, the EU-Australia Agreement, and the EU PNR system.[11] The fact that these instruments are likely to violate the right to privacy is evaluated by taking into account not only the above-mentioned legislative lacuna but also the fact that the Treaty of Lisbon will eliminate the EU pillar structure, consider more extensively the importance of the protection of individual rights in the European Union, and give significant legislative powers to the European Parliament which will be placed on an equal footing with the Council in several areas of EU legislation. This will contribute to the development of the 'democratic nature' of EU institutions.

These circumstances will also produce positive effects for PNR instruments that, once modified, can represent effective tools in the fight against terrorism that are respectful of the right to privacy.

2. The right to privacy: The legal background

2.1. The right to privacy: International law and the European Court of Human Rights' case law

The right to privacy was recognized for the first time at the international level by Article 12 of the 1948 Universal Declaration of Human Rights, which provides: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks'.[12] Subsequently, the wording of this Article was reproduced in Article 17 of the 1966 International Covenant on Civil and Political Rights.[13]

At a regional level, Article 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[14] provides: 'Everyone has the right to respect for his private and family life, his home and his correspondence'. The European Convention provides that the right to privacy can be subjected to some restrictions provided that certain conditions are satisfied. According to Article 8 (2) of the European Convention: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.[15]

The European Court of Human Rights has delivered several decisions on this topic in order to specify the content and the extent of the right to privacy. According to its case law, limitations to the right to privacy are admitted if the restrictive measure in question: 1. is prescribed by law; 2. pursues a legitimate aim; and 3. is necessary in a democratic society in order to pursue that legitimate aim.[16]

In order to satisfy the first condition it is necessary that the restrictive measure has 'some basis in domestic law.'[17] As far as the quality of the law is concerned, it should be compatible with the rule of law, formulated with sufficient precision and 'accessible to the person con-

11 See Sections 4-7, *infra*.
12 Art. 12, Universal Declaration of Human Rights, 10 December 1948.
13 Art. 17, 1966 UN International Covenant on Civil and Political Rights, 16 December 1966.
14 Art. 8, 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950.
15 *Ibid.*, Art. 8, Para. 2.
16 For a detailed analysis of the Court's case law, see S. Sottiaux, *Terrorism and Limitation of Rights: The ECHR and US Constitution*, 2008; see also F. Bignami, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive', 2007 *Chicago Journal of International Law* 8, no. 1, pp. 233-255, in particular pp. 242-249.
17 *Kruslin* v. *France*, [1990] *ECHR* (Ser. A176-A), Para. 27; *Kopp* v. *Switzerland*, [1998-II] *ECHR*, Para. 55.

cerned',[18] in order to enable him 'to regulate his conduct',[19] 'to foresee its consequences for him',[20] and to be protected against 'arbitrary interferences' by public authorities with the right to privacy.[21] In order to assess the necessity of a given measure in a democratic society, the existence of a pressing social need must be evaluated:[22] in particular, it is possible to restrict the right to privacy provided that the measure employed is 'proportionate to the legitimate aim pursued.'[23] States have a 'certain margin of appreciation in assessing whether such a need exists.'[24] The scope of the margin of appreciation enjoyed by the national authorities in the assessment of the proportionality of the measure depends not only 'on the nature of the legitimate aim' of the restriction, but also on 'the nature of the right involved'.[25]

2.2. The processing of personal data and the free flow of information: Council of Europe Convention No. 108 and Directive 95/46/EC

The ongoing growth in the automatic elaboration of personal data that occurred in the 1970s has determined a significant flow of information both at transboundary and intercontinental levels. However, the expansion of the transmission modalities and of the processing of personal data has determined important political and legal debates on the relationship between the protection of privacy and the free flow of information. Until the beginning of the 1980s, the European legal context regarding the protection of personal data and the control of bank data was very fragmentary, and there was no legal uniformity in this particular area.[26]

As a consequence, the Council of Europe and the European Union adopted instruments in order to fill the legislative gap and to guarantee the legal uniformity between states in matters concerning the right to privacy.

In 1981, the Council of Europe adopted the so-called Convention No. 108.[27] The aim of the Convention is to guarantee the privacy of each individual in the 'automatic processing of personal data regarding him.'[28] The Convention has recognized an individual right to privacy and to data protection in the activities concerning the automatic processing of personal data. The Convention identifies the method of personal data transfer which is respectful of the right to privacy, stating that personal data undergoing automatic processing must be: 'a. obtained and processed fairly and lawfully; b. stored for specified and legitimate purposes and not used in a way which is incompatible with those purposes; c. adequate, relevant and not excessive in relation to the purposes for which they are stored'.[29] Furthermore, special categories of data, so-called sensitive data,[30] 'may not be processed automatically', save for certain exceptions.[31]

---

18 *Kruslin*, *supra* note 17, Para. 27; *Kopp*, *supra* note 17 , Para. 55.
19 *Sunday Times* v. *the United Kingdom*, [1979] *ECHR* (Ser. A30), Para. 49.
20 *Kopp*, *supra* note 17, Para. 55; *Amman* v. *Switzerland*, [2000-II] *ECHR*, Para. 50.
21 *Ollson* v. *Sweden*, [1988] *ECHR* (Ser. A130), Para. 61.
22 *Norris* v. *Ireland*, [1988] *ECHR* (Ser. A142), Para. 44; *Dudgeon* v. *The United Kingdom*, [1988] *ECHR* (Ser. A142), Para. 48.
23 *Gillow* v. *The United Kingdom*, [1986] *ECHR* (Ser. A109), Para. 55.
24 *Lingens* v. *Austria*, [1986] *ECHR* (Ser. A103), Para. 39.
25 *Ibid.*, Paras 39-40; *Leander* v. *Sweden*, [1987] *ECHR* (Ser. A116), Para. 59; *Gillow*, *supra* note 23, Para. 55.
26 See D. Blonda, *La Disciplina della Privacy nel Panorama Internazionale*, available online at <http://www.jei.it/approfondimentigiuridici/notizia.php?ID_articoli=516>.
27 1981 COE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981, available online at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>; see also Council of Europe, *Explanatory Report on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Convention Opened for Signature on 28 January 1981*, 1981.
28 Art. 1, COE Convention, *supra* note 27.
29 Art. 5, COE Convention, *supra* note 27.
30 According to Art. 6, COE Convention, *supra* note 27, sensitive data is 'personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life'.
31 Art. 6, COE Convention, *supra* note 27.

However, the Convention has one important gap: its scope covers the sole protection of automatically processed personal data, but it does not include non-automated data.[32]

Directive 95/46/EC[33] has filled this lacuna because it applies to data processed by both automated and non-automated means.[34] Indeed, after having defined personal data as any information concerning an 'identified or identifiable natural person',[35] the Directive affirms the principles regulating the processing of personal data considered as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means'.[36] Principles affirmed in this Directive thus integrate and broaden those affirmed by Convention No. 108.[37] Article 8 of the Directive even excludes the processing of personal sensitive data,[38] providing exceptions in that regard.[39]

With the adoption of Directive 95/46, the European legislation concerning the protection of personal data seemed to be adequate and complete because it, together with Convention No. 108, coherently harmonized the free flow of information and the protection of privacy. However, over the years, these norms have shown their lacunae and their incapacity to face new-world challenges, in the light of the ever-increasing use of automated means, bank data and the strengthening of the EU's anti-terrorism measures.

2.2.1. The Community principles governing the processing of personal data

According to Directive 95/46, Member States must respect the following principles in the processing of personal data: the purpose limitation, the data quality and proportionality principle, and the transparency principle.[40]

Article 6 of the Directive provides that personal data must be 'processed fairly and lawfully (…) and collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'.[41] According to the purpose limitation principle, data must be processed for a defined purpose and its subsequent use, transmission or collection must be in compliance with that purpose.[42] It is thus necessary that the law provides exactly the aims to be achieved through the processing of personal data. The clear formulation of the disposition

32 See Blonda, *supra* note 26.

33 Directive 95/46/EC, *OJ* L 281, 23.11.1995, p. 31. In the doctrine see M. C. Ponthoreau, 'La Directive 95/46 CE du 24 Octobre 1995 Relative à la Protection des Personnes Physiques à l' Égard du Traitement des Données à Caractère Personnel et à la Libre Circulation de ces Données', 1997 *Revue Française de Droit Administratif* 13, no. 1, pp. 125-150; R. Castaño Suárez, 'Directiva 95/46, de 24 de Octubre de 1995, Relativa a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de Éstos. Similitudes y Diferencias con la Ley Orgánica 5/1992, de 29 de Octubre (LORTAD)', 1998 *Noticias de la Unión Europea*, no. 14, pp. 9-15; A. L. Calvo Cravaca *et al*., 'International Data Protection, Privacy and Directive 95/46/EEC', in: J. Basedow *et al*. (eds.), *Aufbruch Nach Europa: 75 Jahre Max-Planck-Institut für Privatrecht*, 2001, pp. 167-182.

34 See European Union, Summaries of Legislation – Protection of personal data, available online at <http://europa.eu/legislation_summaries/information_society/l14012_en.htm>.

35 Art. 2(a), Directive 95/46/EC, *supra* note 33.

36 Art. 2(b), Directive 95/46/EC, *supra* note 33. According to the wording of the Directive these operations can include 'collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

37 Directive 95/46/EC, *supra* note 33, 11th Whereas.

38 Art. 8(1), Directive 95/46/EC, *supra* note 33.

39 Art. 8(2)(a)-(e), (3), (4), Directive 95/46/EC, *supra* note 33.

40 Art. 6, Directive 95/46/EC, *supra* note 33; see also Article 29 Data Protection Working Party, Opinion 8/2007 on the level of protection of personal data in Jersey, WP 141, 9 October 2007, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp141_en.pdf>, p. 6; Commission of the European Communities, Staff Working Document, The application of Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, 20 October 2004, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1322_en.pdf>, p. 4.

41 Art. 6(b), Directive 95/46/EC, *supra* note 33.

42 See Article 29 Data Protection Working Party, Opinion 9/2007 on the level of protection of personal data in the Faroe Islands, WP 142, 9 October 2007, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp142_en.pdf >, p. 5.

is aimed at avoiding the identification of purposes so wide as to allow unjustified intrusions into the private life of the individual subject to the treatment.

The application of the purpose limitation is strictly related to the data quality and proportionality principle. According to Article 6 of the Directive, the personal data must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected (…) or further processed (…), accurate and, where necessary, kept up to date'.[43] The scope of the proportionality principle, which is one of the general principles of Community law, has also been elaborated by the Community courts. It requires that measures adopted by Community institutions 'should not exceed the limits of what is appropriate and necessary in order to attain the legitimate objectives (…), and where there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued'.[44]

According to the transparency principle, individuals must be given precise and detailed information concerning the aims of the collection and processing of data regarding them as well as other information necessary to guarantee the fairness of the operations.[45]

2.3. The structural incapacity of the European Union to protect the right to personal data protection, and Council Framework Decision 2008/977/JHA

The situation involving a legislative lacuna examined above is caused by the structural incapacity of the European Union to protect, as a whole, the right to have personal data protected. The structure of the European Union, as outlined by the Maastricht Treaty,[46] is based on three pillars: 1. the Community pillar, corresponding to the European Communities (first pillar); 2. the common foreign and security policy (CFSP), provided for by Title V of the EU Treaty (second pillar); 3. police and judicial cooperation in criminal matters, provided by Title VI of the EU Treaty (third pillar).[47]

Directive 95/46 is not to be applied to the processing of personal data in the course of activities falling under the second and third pillars.[48] This significant legislative lacuna has deprived individuals of the full protection of their right to privacy, which has been limited by several anti-terrorism measures adopted by the European Union in the second[49] and third pillars. Until 2008, European Union activities falling under the second and third pillars were not completely supported by norms effectively protecting the right to data protection.[50] In this regard, the adoption in 2008 of the Council Framework Decision on the protection of personal data processed within the framework of police and judicial cooperation in criminal matters between

---

43 Art. 6(c), (d), Directive 95/46/EC, *supra* note 33.

44 Case C-331/88, *Fedesa and Others*, [1990] *ECR* I-4023, Para. 13; Case T-13/99, *Pfizer Animal Health* v. *Council of the European Union*, [2002] *ECR* II-3305, Para. 411; Case T-70/99, *Alpharma Inc.* v. *Council of the European Union*, [2002] *ECR* II-3495, Para. 324.

45 Arts. 10, 11, Directive 95/46/EC, *supra* note 33; see also Opinion 9/2007, *supra* note 42, p. 5.

46 1992 Treaty on European Union, 7 February 1992, *OJ* C 191, 29.7.1992.

47 See B. Conforti, *Diritto Internazionale*, 2002, p. 164; F. Pocar, *Diritto dell'Unione Europea e delle Comunità Europee*, 2004, p. 56.

48 Art. 3(2), Directive 95/46/EC, *supra* note 33.

49 See Council Common Position 2001/931/CFSP, *OJ* L 344, 28.12.2001, p. 93; and Regulation (EC) no. 2580/2001 implementing this Council Common Position, *OJ* L 344, 28.12.2001, p. 70. The European Union has adopted the so-called smart sanctions, imposing travel bans, embargoes and the freezing of assets on individuals or entities included in certain EU lists. On the topic of targeted sanctions and on the problems they raise as to fundamental rights and freedoms, see G. Ziccardi Capaldo, 'Editorial: Fighting Global Terrorism: Through Global Enforcement Mechanisms', in: G. Ziccardi Capaldo (ed.), *The Global Community. Yearbook of International Law and Jurisprudence*, 2004, pp. xv-xxvii, in particular pp. xxiii-xxv; G. Ziccardi Capaldo & M. Nino, 'Globalization of Law Enforcement Mechanisms: Issues of Legality and Legitimacy', in: M. Cherif Bassiouni (ed.), *International Criminal Law, Vol. II - Multilateral and Bilateral Enforcement Mechanisms*, 2008, pp. 49-71; G. Ziccardi Capaldo, *The Pillars of Global Law*, 2008, p. 285.

50 A. Scirocco, *The Lisbon Treaty and the Protection of Personal Data in the European Union*, available online at <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2008/08-09-19_Scirocco_Lisbontreaty_DP_EN.pdf>, p. 2.

the Member States is to be welcomed.[51] This decision, which forms part of the third pillar, represents a fundamental tool in order to establish and develop an area of freedom, security and justice.[52] It provides common standards regarding the processing and protection of personal data processed for purposes of preventing and fighting crime.[53] The purpose of the Framework Decision is 'to ensure high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters, provided for by Title VI of the Treaty on European Union, while guaranteeing a high level of public safety'.[54] As a result, the Framework Decision is aimed at balancing two important interests: 1. protecting public safety, by increasing and intensifying the police and judicial cooperation between the Member States in criminal matters, and 2. defending personal data processed in activities falling under the third pillar. According to the European Data Protection Supervisor (EDPS), these interests can coexist because an effective protection of personal data can improve and reinforce the police and judicial cooperation.[55] The Framework Decision is intended to fill the abovementioned lacunae in the European Union legal system: first, it assures that the general principles of the data protection provided for by Directive 95/46 and Convention No. 108 are applied within the area of the third pillar;[56] second, it provides common rules defining those principles.[57] Indeed, according to Article 3 of the Framework Decision: 'Personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes (…) and may be processed only for the same purpose for which data were collected. Processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected'.

The Framework Decision covers not only the exchange of personal data between Member States and EU authorities but also the transfer of those data to third States[58] or to private parties in Member States.[59] According to Article 13 of the Framework Decision, Member States can transmit personal data to third States provided that: '(c) the Member State from which the data were obtained has given its consent to transfer (…); and (d) the third State (…) ensures an adequate level of protection for the intended data processing.'[60]

As to the relationship with previously adopted acts of the Union, the Framework Decision provides that the acts, adopted according to Title VI of the Treaty on European Union prior to the date of the entry into force of the Framework Decision, containing specific provisions on the protection of personal data exchanged or processed pursuant to those acts, prevail over the norms

51 Council Framework Decision 2008/977/JHA, *OJ* L 350, 30.12.2008, p. 60.

52 Second opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, 29 November 2006, *OJ* C 91/9, 26.4.2007, also available online at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2006/06-11-29_data_protection_EN.pdf>, Point 7; Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, 27 April 2007, *OJ* C 139/1, 23.6.2007, also available online at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-04-27_3dpillar_3_EN.pdf>, Point 7.

53 Council Framework Decision 2008/977/JHA, *supra* note 51, 3rd Whereas.

54 *Ibid.*, Art. 1.

55 Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM(2005) 475 final), 19 December 2005, *OJ* C 47/27, 25.2.2006, also available online at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2005/05-12-19_data_protection_EN.pdf>, Point 5.

56 *Ibid.*, Points 24, 25, 47.

57 *Ibid.*, Points 25, 47.

58 Council Framework Decision 2008/977/JHA, *supra* note 51, Art. 13.

59 *Ibid.*, Art. 14.

60 *Ibid.*, Art. 13.

of the Framework Decision.[61] As far as the relationship between agreements with third States is concerned, Article 26 provides that the Framework Decision 'is without prejudice to any obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements with third States existing at the time of adoption of this Framework Decision.'[62] However, it is provided that in the application of those agreements 'the transfer to a third State of personal data obtained from another Member State shall be carried out' in compliance with Article 13 of the Framework Decision.[63]

Although the Framework Decision is very important, being the first instrument intended to provide for the protection of personal data in the third pillar, some scholars[64] and the EDPS have rightly maintained that it does not offer an adequate and overall protection of personal data. According to the EDPS, the Framework Decision has some lacunae. First of all, it concerns only the exchange of personal data between Member States and EU authorities, but it does not cover domestic data.[65] Furthermore, in the opinion of the EDPS, the Framework Decision should be improved because it does not assure an adequate level of protection for the transfer of personal data to third States 'according to a common EU standard' and does not limit 'the purposes for which personal data may be further processed' in compliance with the principles contained in Directive 95/46.[66]

3. The new EU institutional architecture provided for by the Treaty of Lisbon

The Treaty of Lisbon, which was signed on 13 December 2007 and has entered into force on 1 December 2009,[67] marks an important turning point for strengthening the protection of rights and fundamental freedoms in the European Union, and in particular the protection of personal data. It amends the current EU and EC treaties and renames the latter as the Treaty on the Functioning of the European Union.

The elimination of the structure of the pillars allows European institutions to carry out a more unitary and coherent activity aimed at protecting personal data as a whole. The end of the pillar structure could also permit, through an amendment of Directive 95/46, the application of this Directive in other important areas regarding the fight against terrorism, such as the common foreign and security policy, and police and judicial cooperation in criminal matters.[68]

Furthermore, the Treaty of Lisbon will introduce the Charter of Fundamental Rights into Community primary law,[69] making its provisions legally binding. This will strengthen the values and principles on which the European Union is based. In this regard, it is important to recall Article 8 of the Charter of Fundamental Rights of the European Union, which explicitly recog-

61 Council Framework Decision 2008/977/JHA, *supra* note 51, 39th Whereas, Art. 28.
62 *Ibid.*, 38th Whereas, Art. 26.
63 *Ibid.*
64 See P. De Hert & V. Papakonstantinou, 'The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters. A Modest Achievement However not the Improvement Some Have Hoped For', 2009 *Computer Law & Security Review* 25, no. 5, pp. 403-414.
65 EDPS Press Release, *EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step*, 28 November 2008, available online at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2008/EDPS-2008-11_DPFD_EN.pdf>.
66 *Ibid.*
67 2007 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13 December 2007, *OJ* C 306, 17.12.2007.
68 See Scirocco, *supra* note 50, p. 3; D. Alonso Blas, *First Pillar and Third Pillar: Need for a Common Approach on Data Protection*, available online at <http://www.law.ed.ac.uk/file_download/communities/92_article%20dab%20first%20pillar%20and%20third%20pillar%20april%202008.doc>, p. 15.
69 Treaty of Lisbon, *The Treaty at a Glance*, available online at <http://europa.eu/lisbon_treaty/glance/index_en.htm>, Para. 3.

nizes the right to the protection of personal data.[70] This disposition is very important, because it classifies the right to the protection of personal data as an autonomous right, as distinguished from the right to respect for private and family life provided for by Article 7 of the same Charter.[71] Furthermore, Article 16 of the Treaty on the Functioning of the European Union not only recognizes the importance and the autonomy of the right to protection of personal data, but it also provides that the Council and the Parliament will establish, through the ordinary legislative procedure and thus on an equal footing, common rules aimed at protecting individuals' privacy.[72] Finally, the Treaty of Lisbon gives a fundamental legislative role to the European Parliament. The agreement, extending the co-decision procedure in several important areas, such as areas of justice, security and freedom, and substituting the requirement of unanimity with the qualified majority system for the adoption of Community acts, places the European Parliament on the same level as the Council and makes Community legislative activity more democratic.

4. The Agreements concluded between the European Union and the United States on the transfer of personal PNR data

4.1. The United States anti-terrorism legislation on the security of air transport: Problems of compliance with Community law

After the terrorist attacks of September 11, 2001, the United States adopted important measures, both of a repressive and preventive nature, aimed at neutralizing the terrorist threat.[73] In the attempt to assure the efficacy of the counter-terrorism measures, the US administration considered it of fundamental importance to control and analyze the flow of personal data relating to air passengers on flights directed to or arriving from the United States.

In November 2001, the United States adopted legislation enhancing border security that obliged each air carrier, operating passenger flights directed to or arriving from the United States, to provide the United States Bureau of Customs and Border Protection (CBP) with electronic access to PNR data present in the automated reservation system of the air carriers.[74]

The problems of compatibility between US legislation and Community norms protecting individuals' privacy were mainly raised by the Article 29 Data Protection Working Party, the European Parliament and the European Commission.

---

70 2000 European Union Charter of Fundamental Rights, *OJ* C 361/1, Art. 8, also available online at <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

71 *Ibid.*, Art. 7. See S. Rodotà, *Intervista su Privacy e Libertà*, 2005, p. 19. According to Art. 52 of European Union Charter of Fundamental Rights (*supra* note 70), both the right to privacy and the right to the protection of personal data can be limited, provided that the limitations are 'provided for by law (…) respect the essence of those rights and freedoms and the principle proportionality, and are necessary and genuinely meet objectives of general interest recognised by the Union'.

72 Art. 16 Treaty on the Functioning of the European Union, *OJ* C 115/47, 9.5.2008. On the importance of this article see Scirocco, *supra* note 50, pp. 2-3.

73 See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), Pub. L. No. 107-56, 115 Stat. 272 (2001); USA Patriot Improvement and Reauthorization Act of 2005 (9 March 2006), Public Law No. 109-177 (2006). For a detailed review of US anti- terrorism legislation see S. W. Becker, '"Mirror, Mirror on the Wall…": Assessing the Aftermath of September 11th', 2003 *Valparaiso University Law Review* 37, pp. 563 *et seq.*; J.A.E. Vervaele, 'The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies', 2006 *European Journal of Law Reform*, no. 1, pp. 137-171. The US administration also considered the practice of extraordinary renditions of vital importance in the fight against terrorism: on this topic see M. Nino, 'The Abu Omar Case in Italy and the Effects of CIA Extraordinary Renditions in Europe on Law Enforcement and Intelligence Activities', 2007 *Revue Internationale de Droit Penal* 78, no. 1/2, pp. 113-141; M. Nino, 'Extraordinary Renditions: The Role of European Security Services in the Fight Against International Terrorism', 2008 *Revue Electronique de l'Association Internationale de Droit Pénal*, available online at <http://www.penal.org/new/publications.php?Doc_zone=PUB&langage=fr&ID_doc=395>.

74 Aviation and Transportation Security Act (ATSA), 19 November 2001 (Public Law 107–71, 107th Congress, 49 USC Section 44909(c)(3) (2001)). In 2002, the US passed legislation concerning border security (Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSV), 5 May 2002).

The Article 29 Data Protection Working Party, by affirming the necessity to reach a proper balance between the security needs and the protection of individual guarantees, and considering the individual's right to protection of personal data as a part of the fundamental rights and freedoms of the individual protected by the European Union,[75] stated that compliance by the air carriers with the US legislation would probably have caused problems in respect of Directive 95/46/EC[76] and expressed concerns as to the level of personal data protection assured in the US.[77]

The European Parliament, criticizing the initial positions of the Commission, invited it to adopt actions in the area of the transfer of PNR data in the US which could be respectful of Community law and of the ECHR. In particular, the European Parliament, expressing doubts about the real effectiveness of the PNR transfer in the fight against international terrorism, underlined that this strategy could have created a system of mass surveillance, in complete violation of principles provided by Directive 95/46/CE, Article 8 of the ECHR, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[78]

The European Commission, which, according to Article 25 of Directive 95/46, is empowered to evaluate whether the transfer of personal data to a third country assures an adequate level of protection of such data under Community law,[79] delayed this examination because of its concerns about the invasiveness of the American legislation and its potential capacity to limit the privacy of individuals. It informed the US authorities that that law could violate some important Community norms concerning personal data protection and computerized reservation systems.[80]

Following the pressures exercised by the Commission, the US authorities postponed the entry into force of the dispositions provided for by the US legislation; at the same time, they did not renounce their intentions to impose sanctions against airlines that failed to comply with the US legislation after 5 March 2003. After that date, several air carriers operating in the European Union provided US authorities with access to their PNR data.

These circumstances created a situation of legal uncertainty for the airlines that were worried both about the possible American sanctions in case of non-compliance with American legislation and the control activities of the European data protection authorities, which could impose sanctions in cases of a failure to comply with the Community law concerning the protection of personal data.

4.2. The transfer of personal data to third countries under Directive 95/46 and the 2004 PNR EU-US Agreement

Article 25 Directive 95/46 identifies the requirements for the transfer of personal data from European Union Member States to third countries, providing that 'the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if (…) the third country in question ensures an adequate level of

75 Article 29 Data Protection Working Party, Opinion 10/2001 on the need for a balanced approach in the fight against terrorism, 14 December 2001, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf>, p. 3. Reference was made in particular to Art. 8 of the Charter of Fundamental Rights of the European Union, *supra* note 70, and to two decisions of the European Court of Human Rights (*Amman*, *supra* note 20, and *Rotaru* v. *Romania*, [2000-V] *ECHR*).

76 Opinion 6/2002, *supra* note 4.

77 Opinion 4/2003 on the Level of Protection ensured in the United States for the Transfer of Passengers' Data, WP 78, 13 June 2003, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp78_en.pdf>.

78 European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights, 13 March 2003, P5_TA(2003)0097; European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA, 9 October 2003, P5_TA(2003)0429.

79 See Section 4.2, *infra*.

80 Reference was made to Directive 95/46/EC, *supra* note 33, and to Regulation (EEC) no. 2299/89 on a code of conduct for computerized reservation systems, *OJ* L 220, 29.7.1989, p. 1, as modified by Regulation (EC) no. 323/1999, *OJ* L 40, 13.2.1999, p. 1.

protection'.[81] The adequacy of the level of protection constitutes the *conditio sine qua non* in order that a third country can obtain a transfer of data from the European Union. The European Commission has the power to examine the level of protection afforded by a third country by taking into account several circumstances concerning the data to be evaluated[82] and deciding whether or not a third country ensures an adequate level of protection required for the transfer of personal data under the procedure provided for by Article 31(2) of Directive 95/46.[83]

On 11 May 2004, the CBP issued Undertakings, which clarified and defined the conditions for the transfer of PNR passengers' data to US authorities, ensuring that such transfer would have taken place in compliance with Community principles concerning individuals' right to privacy.[84] On 14 May 2004 the Commission, by Decision 2004/535/CE, considered that CBP was able to guarantee 'an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States, in accordance with the Undertakings'.[85] In the light of this decision on adequacy, on 17 May 2004, by Decision No. 496/2004, the Council of the European Union approved the conclusion of an Agreement between the European Community and the United States on the processing and transfer of PNR data by air carriers to the United States CBP.[86] Finally, on 28 May 2004, the United States and the European Community definitively signed the Agreement, that entered into force on the date of its signature.[87]

According to the Agreement, the processing and treatment by CBP of PNR personal data was regulated by the Undertakings and US legislation.[88] The Agreement was criticized by the European Parliament, humanitarian associations, and the Article 29 Data Protection Working Party for substantially having bypassed the Community principles concerning the protection of individual privacy and, in particular, for having violated the purpose limitation and the proportionality principles.[89]

As far as the purposes for processing data are concerned, PNR data could be used by CBP in order to 'prevent and combat: 1. terrorism and related crimes; 2. other serious crimes, including organised crime; 3. and flight from warrants or custody for those crimes'.[90] The wording of category no. 2, which was so vague as to encompass criminal activities not properly related with terrorist acts, allowed data transmission not in compliance with the purpose limitation principle.[91] It is fundamental that the fight against international terrorism be limited and defined, and not so wide as to admit unjustified limitations to the right to privacy and fundamental freedoms not provided for by international and Community law.

---

81 Art. 25(1), Directive 95/46/EC, *supra* note 33.
82 *Ibid.*, Para. 2.
83 *Ibid.*, Paras 4, 5, 6.
84 Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP), 11 May 2004 (hereinafter Undertakings).
85 Art. 1, Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, 2004/535/EC, *OJ* L 235, 6.7.2004, p. 11.
86 Council Decision of 17 May 2004 on the conclusion of an 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, 2004/496/EC, *OJ* L 183, 20.5.2004, p. 83.
87 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 142M, 30.5.2004, p. 50.
88 Commission Decision 2004/535/EC, *supra* note 85, Para. 1.
89 See also P. De Sena, 'Esigenze di Sicurezza Nazionale e Tutela dei Diritti dell'Uomo nella Recente Prassi Europea', in: N. Boschiero (ed.), *Ordine Internazionale e Valori Etici, VIII Convegno SIDI, 2003*, pp. 196-268, in particular p. 255; B. Siemen, 'The EU-US Agreement on Passenger Name Records and EC-Law: Data Protection, Competences and Human Rights Issues in International Agreements of the Community', 2005 *German Yearbook of International Law* 47, pp. 629-665.
90 Commission Decision 2004/535/EC, *supra* note 85, 15th Whereas; Undertakings, *supra* note 84, Point 3.
91 See Opinion 4/2003, *supra* note 77, pp. 6-7.

As for PNR data to be transferred, it was provided that the transfer of such data encompasses a list of 34 elements.[92] As a rule, the transmission of sensitive data protected by Article 8 of Directive 95/46 was excluded.[93] Although the original scheme of the Agreement provided for the transfer of 38 PNR data and thus there was a quantitative reduction of the transmissible data, the number and the quantity of the data to be transferred under the 2004 Agreement remained very wide; therefore, the transfer was not adequate and relevant according to the principles enshrined in Article 6 of Directive 95/46.[94]

As to the length of time of the data retention, it was provided that the CBP would keep and access the PNR data of passengers for three years and six months.[95] PNR data that had not been manually accessed during that time period would be destroyed. PNR data that had been manually accessed during that period would remain for a period of eight years in a CBP record file, and be subsequently destroyed.[96] The data retention time appeared not only less effective for investigation purposes, but also excessive and not in compliance with the principle of proportionality.[97]

The method of data transfer chosen was the 'pull' system, according to which US authorities had direct access to air carriers' reservation systems.[98] This system was preferred to the more protective 'push' system, under which the authority requesting PNR data received it from the air carriers, without having direct online access to their databases.[99]

4.3. The European Court of Justice judgment issued in Cases C-317/04 and C-318/04

On 27 July 2004, the European Parliament, supported by the EDPS,[100] brought two actions for annulment under Article 230[101] EC, which were subsequently joined, before the Court of Justice of the European Communities (ECJ) in order to seek the annulment of Council Decision no. 496 and Decision no. 535 on adequacy.[102] In its Opinion of 22 November 2005, Advocate General Léger[103] recommended the annulment of both decisions. He held that the use and processing of PNR data by CBP constitute activities concerning 'public security and State activities in areas of criminal law', and, as such, they were excluded from the scope of Directive 95/46.[104] The fact that PNR data was initially collected for commercial purposes did not exclude that it had been subsequently collected and processed for protecting 'public security' and satisfying 'law-enforcement purposes'.[105] Furthermore, the Advocate General excluded that Article 95 EC could

92 See Undertakings, *supra* note 84, Attachment A.
93 *Ibid.*, Points 9-11.
94 Opinion 4/2003, *supra* note 77, pp. 6-7.
95 Undertakings, *supra* note 84, Point 15.
96 *Ibid.*
97 See Opinion 4/2003, *supra* note 77, p. 8.
98 2004 Agreement, *supra* note 87, Para. 1.
99 See European PNR, Proposal for a Council Framework Decision of 6 November 2007 on the use of Passenger Name Record (PNR) for law enforcement purposes, available online at <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14584_en.htm>.
100 See Peter J. Hustinx (EDPS), Presentation of Annual Report 2004, Introductory Speech at Press Conference: *Building a new institution*, 31 March 2005, available online at <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2005/05-03-31_Annual_report_EN.pdf>, p. 4; EDPS Press Release, *EDPS will support Parliament in PNR-cases before the European Court of Justice*, 31 March 2005, available online at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2005/EDPS-2005-2_ECJ_PNR_EN.pdf>.
101 Art. 230, 1957 Treaty establishing the European Community, 25 March 1957.
102 See notes 85-86, *supra*.
103 See Opinion of Advocate General Léger, 22 November 2005.
104 *Ibid.*, Para. 97. According to Art. 3(2), Directive 95/46/EC, *supra* note 33, the directive is not to be applied to the processing of personal data 'in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (…) and the activities of the State in areas of criminal law'.
105 *Ibid.*, Para. 103.

constitute an appropriate legal basis for the adoption of Council Decision no. 496 because that article concerns measures aimed at realizing 'the establishment and functioning of the internal market',[106] and is thus not aimed at countering terrorism.

In its judgment of 30 May 2006, the ECJ, following the conclusions of the Advocate General, annulled both Council Decision no. 496 and the Decision no. 535 on adequacy.[107] According to the Court, the decision on adequacy involved the processing of personal data not falling within the scope of Directive 95/46 and, as a consequence, it infringed the Community norm itself.[108] As to Council Decision no. 496, the Court held that Article 95 EC could not 'justify the Community competence to conclude the Agreement' between the US and the EU on the transfer of PNR data.[109] As a consequence, the Court ordered the annulment of the Agreement but, at the same time, it preserved the effect of Decision 2004/535 until 30 September 2006.[110]

The ECJ focused its attention on procedural aspects, such as those concerning the scope of Directive 95/46 and the Community competence to conclude an agreement in a specific area under Article 95 TCE. The Court did not draw its attention to other important topics, both substantive and procedural, raised by the European Parliament and examined by Advocate General Leger, such as the effects of the contested decisions on the exercise of the right to privacy of individuals. On the one hand, the judgment of the Court in the short term resulted in the annulment of the Agreement and thus the elimination of the negative effects on the right to privacy arising from the application of that Agreement; on the other hand, the ECJ decision did not contribute to assuring the certainty of the law in the long term as it failed to reach a definitive and clear solution to the problems raised by the Agreement.[111] This orientation created a situation of legal uncertainty that led to the 2007 Agreement, which contains dispositions that, even to a greater extent than before, limit the fundamental principles protecting the right to privacy.

4.4. The 2006 interim Agreement

In October 2006, after the conclusion of the negotiations between the Commission and the United States, the EU Council approved an interim Agreement between the European Union and the US on the processing and transfer of PNR data from the European Union to US authorities.[112] On 19 October 2006, this Agreement replaced the 2004 Agreement, and it should have expired on 31 July 2007 in order to be replaced by a definitive Agreement.[113] The new Agreement did not

106 *Ibid.*, Para. 141.

107 Joined Cases C-317/04 and C-318/04, *European Parliament* v. *Council of the European Union*, [2006] *ECR* I-4721. For an analysis of the judgment see G. Gilmore *et al.*, 'Court of Justice: Joined Cases C-317/04 and C-318/04, European Parliament v. Council and Commission', 2007 *Common Market Law Review*, no. 4, pp. 1081-1099.

108 Joined Cases C-317/04 and C-318/04, *supra* note 107, Paras 59-60.

109 *Ibid.*, Paras 67-69; see also P. de Hert & S. Gutwirth, 'European Data Protection's constitutional project. Its problematic recognition in Strasbourg and Luxembourg', in: S. Gutwirth *et al.* (eds.), *Reinventing data protection?*, 2009, pp. 3-44.

110 Joined Cases C-317/04 and C-318/04, *supra* note 107, Para. 74; see also the reactions of EDPS to ECJ judgment (EDPS Press Release, *PNR: EDPS first reaction to the Court of Justice judgment*, 30 May 2006, available online at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2006/EDPS-2006-8_PNR_EN.pdf>; EDPS, *Newsletter*, no. 4, 1 June 2006, PNR Judgement, available online at <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_4_EN.pdf>, p. 4).

111 Some authors have stated that the ECJ judgment has created a '*lacuna legis*': see E. Kosta *et al.*, 'Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive', 2007 *International Review of Law Computers and Technology* 21, no. 3, pp. 347-362, also available online at <http://www.bileta.ac.uk/Document%20Library/1/Data%20protection%20in%20the%20third%20pillar%20-%20in%20the%20aftermath%20of%20the%20ECJ%20decision%20on%20PNR%20data%20and%20the%20data%20retention%20directive.pdf>, p. 3.

112 Council Decision of 16 October 2006 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, 2006/729/CFSP/JHA, *OJ* L 298, 27.10.2006, p. 27.

113 Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, *OJ* L 298, 27.10.2006, p. 2.

contain the precise indication of the PNR data that was the object of the processing and the transfer, and it retained the 'pull system' as the method of personal data transfer.[114] As to the US authorities empowered to have access to PNR data kept by the air carriers, the Agreement provided that not only the CBP – the only entity entitled to have access to PNR data according to the 2004 Agreement – but also the 'US Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support[ed] it' could have this power.[115] Furthermore, the Agreement established that the processing and transfer of data would have occurred 'in accordance with applicable US laws and constitutional requirements',[116] mentioning only in the 'whereas' clause the Community norms on the protection of privacy.[117]

The vague definition of PNR data to be transferred, the maintenance of a method of data transfer more susceptible to jeopardizing the protection of privacy and the expansion of the entities empowered to have direct access to PNR data kept by air carriers show that the norms of the 2006 Agreement, although they were less precise and detailed than those of the 2004 Agreement, permitted dangerous abuses and facilitated violations of the fundamental freedoms of individuals.[118]

4.5. The 2007 definitive Agreement: The concrete risk of the violation of passengers' privacy

By its Decision of 23 July 2007, the Council of the European Union approved the conclusion of a new Agreement on the processing and transfer of PNR data that replaced the Agreement concluded in 2006.[119] The Agreement consists of the document itself and a US letter to the EU that explains the modalities for the storage, use and transfer of PNR data by Homeland Security.[120]

Title I of this letter specifies the purposes for which US authorities can use PNR data, such as the prevention of and combating '1. terrorism and related crimes; 2. other serious crimes, including organized crime; and 3. flight from warrants or custody for those crimes'.[121] Furthermore, US authorities can use and process PNR data in order to protect 'the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by US law'.[122] The wording of the new Agreement not only retains the structure of the previous Agreement but it also widens these purposes.[123] As also correctly pointed out by the Article 29 Working Party, the Agreement does not provide definitions of 'terrorism-related crime and

114 *Ibid.*, Para. 2.
115 *Ibid.*, 2d Whereas.
116 *Ibid.*, Para. 3.
117 *Ibid.*, 5th Whereas.
118 See also D.R. Rasmussen, 'Is International Travel Per Se Suspicion of Terrorism?: The Dispute Between the United States and European Union over Passenger Name Record Data Transfers', 2008 *Wisconsin International Law Journal* 26, no. 2, pp. 551-590, p. 585.
119 Council Decision of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), 2007/551/CFSP/JHA, *OJ* L 204, 4.8.2007, p. 16.
120 Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), *OJ* L 204, 4.8.2007, p. 16. In the doctrine see S. Adam, 'Quelques Réflexions sur les Relations Entre les Procédures a Priori et a Posteriori d'Examen de Compatibilité des Accords Communautaires Suite à l'Affaire dite de "l'Accord PNR"', 2007 *Cahiers de Droit Europeen* 42, no. 5-6, pp. 657-696; K. Hailbronner *et al.*, 'The Agreement on Passenger-Data Transfer (PNR) and the EU-US Cooperation in Data Communication', 2008 *International Migration* 46, no. 2, pp. 187-197; J. Argomaniz, 'When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms', 2009 *Journal of European Integration/Revue d'Integration Europeenne* 31, no. 1, pp. 119-136.
121 *Ibid.*, Title I, US letter to EU.
122 *Ibid.*
123 See also E. Quillatre, 'The EU-US PNR Agreement: Fight Against Terrorism v. Personal Data Protection', available at <http://digidroit.info/memoires//Elisa/PNR/PNR.html>, p. 10.

serious crimes including organised crimes'.[124] The vagueness of the indicated purposes can legitimize a widespread use of PNR data, not in compliance with the purpose limitation and data quality and proportionality principles. The fact that PNR data can also be used 'in any criminal judicial proceedings, or as otherwise required by US law' is not to be welcomed: in this way, the certainty of law is not assured because US authorities could decide to use and process PNR data for less serious offences than terrorism or organised crime, putting at risk individuals' right to privacy.[125]

As for data elements to be transferred, the 2007 Agreement reduces the quantity of transmissible data from the original 34 elements of the 2004 Agreement to the current 19 elements.[126] Although it seems that, through this reduction, the 2007 Agreement affects the right to privacy less than the 2004 Agreement, paradoxically, the variety of the transmissible data has increased.[127] Furthermore, in an exceptional case the US authorities can use sensitive data, an activity that was excluded under the 2004 Agreement.[128] As a result, the amount of information that US authorities can obtain and process has become very wide and it is not proportionate to the aims pursued by the Agreement.

The 2004 Agreement identified a limited number of agencies within Homeland Security that were entitled to receive PNR data. Instead, the 2007 Agreement provides that DHS can process PNR data received from the European Union and 'treat data subjects concerned by such processing in accordance with applicable US laws',[129] thereby not identifying the specific agencies empowered to have access to PNR data. In this way, a general and disproportionate enlargement of entities entitled to have access to air passengers' personal data is allowed.

Furthermore, the 3½ years of PNR data retention provided for by the 2004 Agreement has been extended to 15 years by the 2007 Agreement. PNR data is retained for seven years in an active database and subsequently moved to a dormant database.[130] This data retention time appears disproportionate and excessive in relation to the purposes to be achieved, raising problems of compliance with the Community principles of proportionality and purpose limitation, as well as with Article 8 of the ECHR.[131]

As to the method of data transfer, the 2007 Agreement has replaced the pull system provided for by the 2004 Agreement with the push system.[132] In this way, US authorities do not have direct access to PNR data, but they can receive it from the air carriers. However, the Agreement provides that the pull system remains in effect whereas, by January 2008, some air carriers cannot apply the push system.[133] The choice of system for data transmission, whose

124 Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, WP 138, 17 August 2007, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_en.pdf>, p. 7; see also EDPS, *Newsletter*, no. 11, 19 September 2007, Article 29 Working Party issues Opinion on PNR Agreement, available online at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_11_EN.pdf>, p. 4.

125 *Ibid.*, pp. 7-8.

126 See 2007 PNR Agreement, *supra* note 120, Title III, US letter to EU.

127 European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, *OJ* C 175E, 10.7.2008, p. 564, Point 18; see also M.R. VanWasshnova, 'Data Protection Conflicts Between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System of Financial Information Exchange', 2007-2008 *Case Western Reserve Journal of International Law*, pp. 827-865, p. 839.

128 See 2007 PNR Agreement, *supra* note 120, Title III, US letter to EU.

129 2007 PNR Agreement, *supra* note 120, Para. 3.

130 *Ibid.*, Title VII, US letter to EU.

131 See Opinion 5/2007, *supra* note 124, p. 13; see also European Parliament resolution of 12 July 2007, *supra* note 127, Point 18; Quillatre, *supra* note 123, p. 11.

132 2007 PNR Agreement, *supra* note 120, Title VIII, US letter to EU.

133 *Ibid.*

application allows a better control of US authorities and a reduced risk to the privacy of passengers, is to be welcomed. Yet, the possible coexistence of the pull and push system not only can legitimize possible violations of the air passengers' right to privacy, but it could also cause a 'distortion of competition between EU air carriers'.[134]

The 2007 Agreement identifies US laws as the exclusive point of reference for the processing and transfer of personal data from the European Union to the United States. According to the Agreement, DHS can process and use PNR data 'in accordance with applicable US laws',[135] and the EU cannot 'interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds'.[136] The dependence of the European Union on US laws constitutes a dangerous signal,[137] also in the light of the fact that – as held by some scholars – there is no 'general framework in the US concerning all processing of personal data'.[138] The Agreement does not take completely into account the existence of differences between Community law and US laws regarding the processing of personal data, giving an exclusive power to US law and administration, and consequently putting at risk the exercise of individual rights protected by the European Union.

The 2007 Agreement, although it formally reduces the number of transmissible data, adopts mainly the push system, provides a system of periodical review of its implementation[139] and for the application of the US Privacy Act to Community citizens, it allows, in a greater way than the 2004 Agreement, a serious limitation of passengers' right to privacy and is not in compliance with Community norms on the right to privacy.[140] As a result, it is necessary that the Agreement be modified through: 1. a clearer definition of the purposes to be achieved; 2. a coherent and adequate evaluation of the data to be transferred; 3. a clear identification of the authorities empowered to receive the data; 4. a uniform application of the push system; and, 5. a more-defined and binding reference to Community principles concerning the right to privacy.

5. The 2005 Agreement on PNR/API data transfer between the European Union and Canada

In 2005, the European Union entered into another important Agreement on PNR/API data transfer, this time with Canada.[141] At the beginning of its negotiation, the Canadian-EU Agreement on the transfer of PNR/API data raised relevant legal problems, such as the difficulty in harmonising the Canadian provisions on personal data transfer with the Community legislation concerning the right to privacy. The proposal for the Agreement, which was subsequently modified following the negative Opinion of the Article 29 Working Party,[142] provided some dispositions not completely in compliance with the right to privacy. Following the negotiations

134 European Parliament resolution of 12 July 2007, *supra* note 127, Point 8.
135 See 2007 PNR Agreement, *supra* note 120, Para. 3.
136 *Ibid.*, Para. 6.
137 See also Rasmussen, *supra* note 118, pp. 588-589.
138 See Quillatre, *supra* note 123, p. 9.
139 2007 PNR Agreement, *supra* note 120, Title X, US letter to EU.
140 Some authors have stated that the 2007 Agreement violates individuals' privacy and contains less guarantees than the 2004 Agreement: see Quillatre, *supra* note 123, pp. 10-12; VanWasshnova, *supra* note 127, p. 839; Rasmussen, *supra* note 118, pp. 588-590.
141 Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, *OJ* L 82, 21.3.2006, p. 14.
142 Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines, WP 88, 11 February 2004, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp88_en.pdf>.

between European Union and Canadian representatives, the Canadian authorities complied with the requirements of the European Union, thereby modifying the original proposals.

According to the Agreement at issue, the transfer and the processing of personal data from the European Union to Canada are regulated by the Commitments of the Canada Border Services Agency (CBSA)[143] and by Canadian national legislation concerning the enhancement of security 'to the extent indicated in the Commitments'.[144] CBSA receives personal data 'under section 107.1 of the Customs Act, paragraph 148(d) of the Immigration and Refugee Protection Act'.[145]

As far as the method of data transfer is concerned, Section 7 of the Commitments has accepted the push system, which allows less abuses and more control over the flow of air passengers' personal data.[146] Air carriers, by transferring data selected by them and not being obliged to allow Canadian authorities to have direct access to their data, can avoid potential violations of individuals' right to privacy.

The Agreement contains a list of 25 data elements to be transferred to the CBSA, but the results are qualitatively very limited.[147] The Commitments excluded within this material '"sensitive data elements" (…) and all "open text" or "general remarks" fields'.[148] This disposition is to be welcomed because it excludes the transmission of sensitive data, thereby complying with Article 8 of Directive 95/46, and it avoids the general transfer of personal data, thus excluding the transmission of 'open categories' of data, which – as recalled by the European Parliament – 'could create confusion …with regard to sensitive aspects of the behaviour of the passenger'.[149] However, although the Article 29 Working Party and European Data Protection Supervisor have welcomed the list of PNR data to be transferred under the Agreement, they have expressed some shared doubts. The former has underlined that not all the data elements to be collected are 'relevant and not excessive' under Community law.[150] The EDPS has stated that the transfer of certain categories of data can give rise to problems as to the protection of the right to privacy.[151]

As to the data retention time, the Commitments provide for a data retention period of 3½ years for personal data concerning a 'person who is not subject to an investigation in Canada'.[152] This term seems to be in compliance with the proportionality and data quality principles provided for by Community law.

As to the transfer of data to other countries, the Commitments provide that 'API and PNR information retained in PAXIS will be shared only with a country that has received an adequacy

143 See Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, 2006/253/EC, *OJ* L 91, 29.3.2006, p. 49, Annex, Commitments by the Canada Border Service Agency in Relation to the Application of its PNR Program.

144 *Ibid.*, 11th Whereas.

145 *Ibid.*, 6th Whereas.

146 See Commitments, *supra* note 143, Section 7.

147 Commission Decision 2006/253/EC, *supra* note 143, Attachement A.

148 Commission Decision 2006/253/EC, *supra* note 143, Attachement A, 'PNR Data Elements Required by CBSA from Air Carriers'; Commitments, *supra* note 143, Section 4.

149 European Parliament Report on the proposal for a Council decision on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data (COM(2005)0200 – C6-0184/2005 – 2005/0095(CNS)), Final A6-0226/2005, available at <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2005-0226&language=EN>, p. 10.

150 Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines, WP 103, 19 January 2005, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp103_en.pdf>, p. 4.

151 Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data (COM(2005) 200 final), *OJ* C 218, 6.9.2005, p. 6, Para. 22. The European Data Protection Supervisor's Opinion made particular reference to category 10 (frequent flyer information) and category 23 (any collected APIS information), which could reveal data the processing of which is not strictly necessary to the fight against terrorism.

152 See Commitments, *supra* note 143, Section 8.

finding under the Directive, or is covered by it'.[153] The necessity that the country receiving the information assures an adequate level of protection for the right to privacy is an important factor that guarantees a flow of information which respects the right to privacy.

The system of privacy protection under Canadian law is substantially adequate, and it is very close to the European system provided for by Directive 95/46 and Article 286 TCE.[154] The independent Office of the Canadian Privacy Commissioner controls CBSA's respect for privacy under the conditions provided for by the Canadian Charter of Rights and Freedoms and the Privacy Act.[155] The Agreement between Canada and the EU on the transfer of API/PNR is to be positively welcomed because it protects passengers' privacy in a better way than the US-EU Agreement does. However, in the light of the transitional character of the decision on adequacy,[156] it is also necessary that in the case of any renewal or renegotiation, the new Agreement primarily respects air passengers' right to privacy.[157]

First of all, the new Agreement should provide a more extensive definition of the purposes for which the transfer of the personal data of passengers is allowed. Section 2 allows the transfer of data relating to persons having a 'relationship with terrorism or terrorism-related crimes, or other serious crimes, including organized crime, that are transnational in nature'.[158] The Article 29 Working Party has affirmed that those purposes are well defined and have 'a clear relationship with fighting acts of terrorism'.[159] The wording of Section 2 is not in compliance with the Community principle of purpose limitation, because – as is also explained by EDPS – it has not 'limited the purpose of the data processing to terrorism, but extended the purposes to other serious crimes'.[160] The term 'serious crime' is so vague that it allows CBSA to use and process data for purposes not properly related to terrorism.[161] In this way, the right to privacy could be jeopardised because the unclear definition of the purposes according to which the transfer of PNR data is admitted can legitimate dangerous abuses by Canadian authorities. Furthermore, certain categories of data such as 'frequent flyer information' and 'APIS information', whose processing is not necessary and not in compliance with the principles of proportionality and purpose limitation, should be deleted from the list of PNR to be transferred.

6. The 2008 Agreement on EU-sourced PNR data transfer between the European Union and Australia

After having concluded the abovementioned Agreements with the United States and Canada on the transfer of PNR data,[162] on 30 June 2008 the European Union entered into an Agreement[163]

153 *Ibid.*, Section 18.
154 European Parliament Report, Final A6-0226/2005, *supra* note 149, p. 10.
155 Commission Decision 2006/253/EC, *supra* note 143, 22nd Whereas.
156 On this issue see P. Hobbing, *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, 2008, available online at <http://shop.ceps.eu/BookDetail.php?item_id=1704>, p. 35.
157 The decision on adequacy has a temporary nature and, according to Art. 7 of the Commission Decision 2006/253/EC, *supra* note 143, it provides: 'this Decision shall expire three years and six months after the date of its notification, unless extended in accordance with the procedure set out in Art. 31(2) of Directive 95/46/EC'.
158 See Commitments, *supra* note 143, Section 2.
159 Opinion 1/2005, *supra* note 150, p. 4.
160 Opinion of the European Data Protection Supervisor, *supra* note 151, Para. 24; in this sense see also Hobbing, *supra* note 156, p. 36.
161 See Hobbing, *supra* note 156, p. 36.
162 See Sections 4-5, *supra*.
163 Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, *OJ* L 213, 8.8.2008, p. 49; see also Council Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service, *OJ* L 213, 8.8.2008, p. 47.

with Australia. As for the scope of application of the Agreement, the Australian customs service can require and obtain only EU-sourced PNR data concerning passengers 'travelling to, from or through Australia'.[164]

According to this Agreement, the transfer and process of European Union-sourced PNR data by air carriers to the Australian customs service is governed by Australian legislation.[165] The Article 29 Working Party has recognized that Australian legislation on privacy is able to guarantee an adequate level of protection for the privacy of individuals, because it respects individual rights and fundamental freedoms in compliance with Community law.[166] Although the Agreement contains some norms protecting the right to protection of personal data and has been welcomed by the Australian authorities,[167] it can be considered to allow the Australian customs service to limit, in an unjustified way, individuals' right to privacy.

As to the purposes of processing the data, the Australian customs service can process European Union-sourced PNR data, in order to prevent and contrast: '(i) terrorism and related crimes; (ii) serious crimes, including organised crime, that are transnational in nature; (iii) flight from warrants or custody for crimes described above.'[168] Furthermore, PNR data can also be processed where this is necessary 'for the protection of the vital interests of the data subject or other persons'[169] or where it is 'required by court order or Australian law'.[170] In this way, the Australian customs service is authorized to process and transfer PNR data for purposes not properly related to the prevention of and combating terrorism. The indication of these broad purposes is neither contained in the 2007 PNR EU-US Agreement nor in the 2005 PNR/API EU-Canada Agreement. As a result, the wording of the abovementioned dispositions is so wide as to allow unjustified, inadequate and disproportionate PNR data processing not in compliance with the fundamental purpose limitation principle.[171]

As to the data elements to be collected and processed, the Agreement contains a list of 19 elements which are very close to the catalogue of PNR data provided for by the 2007 PNR EU-US Agreement:[172] it allows excessive and disproportionate data transmission which does not respect the principle of proportionality. However, a positive element contained in the Agreement is represented by the fact that the transmission of sensitive data is excluded.[173]

As far as the data retention time is concerned, the Agreement provides a comprehensive 5½-year term of duration.[174] Generally, this data retention period could be considered adequate; however, the wide purposes for which PNR data can be processed mean that the system is not clearly defined even with respect to the data retention time;[175] as a result, the risk of violating individuals' right to personal data protection can be very high.

---

164 *Ibid.*, Annex, Para. 1.
165 *Ibid.*, 8th Whereas.
166 Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines, WP 85, 16 January 2004, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp85_en.pdf>, p. 13.
167 Australia and the EU Sign Passenger Name Record (PNR) Agreement, available online at <http://pr.euractiv.com/node/4104>.
168 Art. 5(1), 2008 EU-sourced PNR data Agreement, *supra* note 163.
169 *Ibid.*, Art. 5(2).
170 *Ibid.*, Art. 5(3).
171 See also the European Parliament recommendation of 22 October 2008 to the Council concerning the conclusion of the Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, 22 October 2008, available online at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0512+0+DOC+XML+V0//EN>, lett. (f)-(g).
172 2008 EU-sourced PNR data Agreement, *supra* note 163, Annex, Para. 9.
173 *Ibid.*, Para. 10.
174 According to Para. 12 of the Annex to the Agreement: 'Customs shall retain EU-sourced PNR data for no more than three-and-a-half years after the date of receipt of the PNR data by Customs, after which time the data may be archived for two further years.'
175 See European Parliament recommendation of 22 October 2008, *supra* note 171, lett. (n).

As to the disclosure of EU-sourced PNR data by the Australian customs service, the Agreement identifies two forms of disclosure: the disclosure within the Australian Government and the disclosure to third-country governments. As to the former, it is provided that the Australian customs service can transfer PNR data, only when anonymised, to specified Australian Government departments and agencies.[176] This disposition is to be welcomed, because it protects the right to privacy of air passengers, avoiding their identification and maintaining their anonymity.[177] As far as the disclosure to third-country governments is concerned, the Agreement provides that customs can decide to transfer PNR data to certain third-country government authorities on a case-by-case analysis.[178] This norm does not clearly define the criteria and the requisites according to which the disclosure of PNR data to third countries is admitted, and does not make reference to the criterion of the appropriateness of the level of protection guaranteed by a third State. As a consequence, it can legitimate abuses by the Australian customs service that could be empowered to violate passengers' right to personal data protection.

However, there are some norms provided by the Agreement which adequately protect the right to privacy of passengers. First of all, according to Article 7 of the Agreement: 'Australia shall provide a system, accessible by individuals regardless of their nationality or country of residence, for seeking access to, and correction of, their own personal information.'[179] The fact that the Agreement is to apply to all EU citizens without any discrimination is an important element. Furthermore, the existence of a system providing protection for passengers' right to privacy and able to receive claims by individuals is to be welcomed. Finally, under Article 9 of the Agreement 'Australia and the EU shall periodically undertake a joint review of the implementation of this Agreement, including the data protection and data-security guarantees, with a view to mutually assuring the effective implementation of the Agreement.'[180] The fact that the EU can be represented by data-protection and law enforcement authorities in the joint review of the Agreement's implementation shows that this procedure is democratic and respects the right to privacy of individuals; however, as has also been reminded by the European Parliament, the Agreement does not provide a precise deadline for this review.[181]

The Agreement between Australia and the European Union on the transfer and processing of European Union-sourced PNR data contains more guarantees than the 2007 USA-EU Agreement does. This is also due to the fact that, unlike the United States, Australia has uniform legislation protecting the right to privacy of individuals. However, it is necessary that the EU-Australia Agreement be modified in order to better protect passengers' right to personal data protection. First of all, the purposes for which the processing of PNR data is allowed should be more limited and the list of PNR data to be transferred should be reduced; in this way, the processing and disclosure of PNR data could respect the purpose limitation and proportionality principles. Second, the criteria according to which the transfer of personal data to third countries is allowed should be more defined: in particular, the Agreement should make reference to the adequate level of protection assured by a third State. Third, it is necessary that a definite deadline for the joint review of the implementation of the Agreement be determined.

176 2008 EU-sourced PNR data Agreement, *supra* note 163, Annex, Paras 2, 5; Schedule to the Annex; see also European Parliament recommendation of 22 October 2008, *supra* note 171, lett. (i).
177 *Ibid.*
178 2008 EU-sourced PNR data Agreement, *supra* note 163, Annex, Para. 6.
179 Art. 7(1)(2), 2008 EU-sourced PNR data Agreement, *supra* note 163.
180 *Ibid.*, Art. 9.
181 See European Parliament recommendation of 22 October 2008, *supra* note 171, lett. (l).

7. The creation of an EU PNR System: The 2007 proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes

The European Union, considering that PNR data collection is an essential tool in effectively fighting international terrorism and organised crime, is going to equip itself with a system of general surveillance over such data in the European Union. On 25 March 2004, by adopting the Declaration on combating terrorism, the European Council invited the European Commission to bring forward a proposal for a common EU approach to the use of passenger data for border and aviation security and other law enforcement purposes.[182] In November 2007, the European Commission presented a proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes (hereinafter 'the proposal').[183] The proposal has been carefully examined by the Article 29 Working Party and by the European Data Protection Supervisor, who have criticized it.

The proposal is aimed at harmonising the dispositions of the Member States concerning the duties of air carriers, providing flights to or from the European Union, to transfer PNR data to the Member States' authorities.[184] Currently, there are a few EU Member States that have laws and regulations establishing a system for the transfer and processing of PNR data from air carriers to the competent authorities.[185] Although the attempt to provide unitary norms in the European Union dealing with the processing of PNR data for combating terrorism and organised crime is a welcome development, this proposal contains dispositions which are very similar to some norms of the PNR EU-USA Agreement and – as recalled by EDPS – is going to be applied to all passengers, regardless of whether they 'are under investigation or not'.[186]

The proposal integrates the dispositions provided for by Directive 2004/82/EC on the obligation of carriers to communicate API data to the competent authorities.[187] According to the proposal, the collection of PNR data is a much more effective tool in the fight against international terrorism than the collection of API data.[188] This evaluation is strictly connected to the ambitious purposes of the proposal: it is aimed not only at identifying known terrorists but also at 'carrying out risk assessments of the persons, obtaining intelligence and making associations between known and unknown people'.[189] The aims of the measures provided by the proposal are thus the identification of both known and unknown persons who could be potential criminals or terrorists.[190] However, the proposal does not specify in which manner data will be collected and processed for carrying out these risk assessments.[191]

---

182 See European Council, Declaration on Combating Terrorism, 25 March 2004, available online at <http://consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf>, p. 8.

183 Proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes, SEC(2007) 1422, SEC(2007) 1453, available online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0654:FIN:EN:PDF>.

184 Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, *OJ* C 110, 1 May 2008, p. 1.

185 In 2004, the United Kingdom adopted the Semaphore Project, which is a pilot scheme through which large amounts of data concerning air passengers are stored and used to help intelligence agencies in the fight against some forms of crime, including terrorism and organised crime. On this system see H.M. Government, 'Countering International Terrorism: The United Kingdom's Strategy' (July 2006), available online at <http://www.fco.gov.uk/resources/en/pdf/contest-report>.

186 Opinion of the European Data Protection Supervisor, *supra* note 184, Para. 30.

187 See Directive 2004/82/EC, *supra* note 5.

188 Proposal, *supra* note 183, Explanatory Memorandum, p. 3.

189 *Ibid.*

190 Opinion of the European Data Protection Supervisor, *supra* note 184, Para. 15.

191 Joint Opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, adopted by Article 29 Data Protection Working Party and Working Party on Police and Justice, WP 145, 5 December 2007, available online at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp145_en.pdf , p. 7.

The proposal is based on a decentralized system according to which air carriers are required to transfer PNR data to Passenger Information Units (PIUs) that are designated by each Member State.[192] Article 4 of the proposal provides that Member States 'shall adopt a list of competent authorities' empowered to receive PNR data from the PIUs. Air carriers can also designate intermediaries that have the task of transmitting data to the competent PIUs.[193] The proposal is too generic, because it does not provide precise information on PIUs, intermediaries and other authorities. These dispositions could cause legal uncertainty and a heterogeneous enforcement of the PNR system in the Member States, considering that each Member State's national legislation provides different powers and competence to law enforcement authorities.[194] Accordingly, it is necessary that the proposal better defines the competences and duties of intermediaries, PIUs and other competent authorities.[195]

According to Article 8 of the proposal, the transfer of PNR data to law enforcement authorities of third countries is allowed, provided that those authorities use the data in order to prevent and combat terrorism and organised crime and that the third country does not transfer the data 'to another third country without the express consent of the Member State'.[196] As reiterated by the European data authorities, the proposal does not specify the conditions under which a Member State can express its consent and does not make reference to the necessity that the third country must assure an adequate level of protection under Article 25 of Directive 95/46.[197]

As to the data to be transferred, the proposal provides that air carriers should transfer 19 PNR data elements to the competent authorities of the Member States. The number and the nature of PNR data to be transferred according to the proposal are very similar to the data provided by the EU-USA Agreement. The transfer of a such relevant number of data elements, which gives competent authorities wide control and surveillance powers concerning the private lives of individuals, is a measure which is neither necessary to combat international terrorism nor proportionate to the aims pursued by the proposal.[198]

As to the method of data transfer, the proposal provides that air carriers transmit PNR data using the push method, which ensures an adequate level of control over passengers' privacy by air carriers. However, if air carriers are not provided with electronic systems to use this method, the proposal allows the PIUs to have direct access to data through the 'pull' method, which is a method that does not entirely respect the right to privacy.[199]

As to the data retention time, Article 9 of the proposal provides a PNR data retention period of five years; once this term expires, the proposal states that data 'shall be kept for a further period of eight years', during which the data can be processed and accessed according to specified conditions.[200] This 13-year term, very close to the 15-year term provided for by EU-US Agreement, appears to be excessive and disproportionate, and as such does not adequately protect the right to privacy of individuals.

---

192 Art. 3, Proposal, *supra* note 183.
193 Art. 6, Proposal, *supra* note 183.
194 Opinion of the European Data Protection Supervisor, *supra* note 184, Para. 73.
195 In this sense see the Opinion of the European Data Protection Supervisor, *supra* note 184, Para. 73.
196 Art. 8, Proposal, *supra* note 183.
197 Joint Opinion, *supra* note 191, p. 3; Opinion of the European Data Protection Supervisor, *supra* note 184, Paras 76-77; Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, available online at <http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf >, p. 8, Para. 31.
198 See also the Opinion of the European Data Protection Supervisor, *supra* note 184, Para. 95.
199 See European PNR, Proposal for a Council Framework Decision of 6 November 2007 on the use of Passenger Name Record (PNR) for law enforcement purposes, *supra* note 99.
200 Art. 9, Proposal, *supra* note 183.

The proposal provides for a mass surveillance system of EU passengers' privacy, it does not adequately respect the purpose limitation and proportionality principles and it may violate the right to privacy of individuals.[201] The proposal's attempt to harmonise EU Member States' legislation regarding the transfer of PNR data is to be welcomed because the necessity to make homogenous the processing of such data in the EU is an important element in order to guarantee the certainty of the law and the rule of law. However, there are several doubts about the effectiveness, the proportionality and the necessity of the measures provided by the proposal, even in light of the unclear formulation of the norms contained therein. It is necessary that the proposal be modified following certain guidelines, in order to ensure a proper and uniform application of the law in EU Member States and, at the same time, to protect effectively the right to privacy of individuals in compliance with Community law.

First of all, European institutions should demonstrate unequivocally the necessity to collect PNR data.[202] Second, the measures provided by the proposal should also take into account the existing Community systems and legislation aimed at controlling the flow of persons,[203] in particular Directive 2004/82.[204] This Directive has still not been fully implemented in EU Member States, and it has not demonstrated that the collection of API data is an inadequate tool in order to fight international terrorism.[205] As a result, it is necessary to eliminate the obstacles to the implementation of Directive 2004/82 and to understand the real usefulness of API data in the fight against terrorist threats. Only after these evaluations, will it be possible to realize the real and concrete importance of the collection of PNR data in the fight against terrorism and organised crime, and, consequently, to create a more balanced PNR EU system that can respect passengers' right to privacy. Furthermore, the proposal should reduce not only the number of PNR data elements to be transferred, providing for only the transmission of essential PNR data that can be necessary in the fight against terrorism, but also the data retention period, by identifying a duration (from 2 to 3½ years) that can balance the protection of privacy with the necessity to protect the Community from a terrorist threat. The proposal should identify the push method as the exclusive method of PNR data transmission. Finally, the proposal should allow data transfer to a third country on condition that the receiving country ensures an adequate level of protection. Following these guidelines, the Council Framework Decision on the use of PNR data for law enforcement purposes could be an important and essential tool in order to effectively combat terrorism, because it would also respect the Community disposition on the right to privacy and the fundamental principles of proportionality and purpose limitation.

8. Conclusions and perspectives: The necessity to modify the existing PNR instruments in light of the Treaty of Lisbon

PNR Agreements concluded by the European Union on the transfer of PNR data and the proposal for a Council Framework Decision are tools that, on the one hand, pursue a legitimate purpose,

201 Joint Opinion, *supra* note 191, p. 13.

202 In this sense see Opinion of the European Union Agency for Fundamental Rights, *supra* note 197, p. 5, Para. 16; see also MEPs voice serious criticism at EU PNR scheme, available online at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+IM-PRESS+20081119IPR42567+0+DOC+PDF+V0//EN&language=EN>.

203 The European Union Agency for Fundamental Rights (in the Opinion, *supra* note 197, Para. 49) and the EDPS (in the Opinion, *supra* note 184) both make reference to the VISA System (Council Decision of 8 June 2004, *OJ* L 213, 15.6.2004, p. 5) and to the Schengen Information System (Council Decision 2007/533/JHA, *OJ* L 205, 7.8.2007, p. 63).

204 Opinion of the European Data Protection Supervisor, *supra* note 184, Para. 49.

205 Joint Opinion, *supra* note 191, p. 6.

such as combating terrorism, but, on the other hand, they do not adequately protect individuals' right to privacy.

The changes introduced by the Treaty of Lisbon will have significant effects on EU anti-terrorism activities and policies, and, in particular, on PNR Agreements adopted by the European Union, as well as on the proposal for a Council Framework Decision. The recognition of an important value such as the protection of personal data in the EU legal system and the attribution of strong decisional powers to the European Parliament will facilitate significant legal changes to these tools, especially in the light of the fact that the European Parliament has often criticized PNR Agreements as exclusive and important tools in the fight against terrorism. In addition, PNR instruments have been adopted by the European Union without fully taking into account the recommendations of the European Parliament, which is a Community institution that is very mindful of the protection of the rights and fundamental freedoms of EU citizens.[206] Through the changes provided for by the Treaty of Lisbon, the European Parliament can control and supervise Agreements concluded by the European Union in areas of justice and the police that could violate individuals' privacy, which would better assure the protection of the right to personal data.[207]

The solutions proposed in this article (a re-elaboration of the EU Agreements with the United States, Canada and Australia, and a more adequate reconsideration of the proposal for a Council Framework Decision) are sensitive concerning the protection of personal data and its coherent integration into the new institutional architecture and legal background introduced by the Treaty of Lisbon, which attempts to counterbalance the protection of privacy with the necessity to counter terrorism.[208]

In conclusion, the Treaty of Lisbon, which has recently entered into force, will attain the appropriate balance between individuals' right to personal data protection and the collective necessity of countering international terrorism in PNR matters.[209] It will provide the European Union with the legislative background and modern institutions to face the new challenges of the world (such as combating terrorism) and to satisfy citizens' requests.[210]

206 See European Parliament resolution of 12 July 2007, *supra* note 127, Point 2. The Parliament in its Resolution concerning the Agreement with Canada did not approve the conclusion of that agreement (European Parliament legislative resolution on the proposal for a Council decision on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data, *OJ* C 157E , 6.7.2006, p. 464, Point 1).

207 In this sense see Alonso Blas, *supra* note 68, p. 17; Scirocco, *supra* note 50, p. 5.

208 See also the Opinion of the European Data Protection Supervisor, *supra* note 184, Para. 129.

209 On the balance between the protection of individual fundamental freedoms and the necessity to fight international terrorism, see G. Ziccardi Capaldo, 'Terrorismo Globale e Diritti Umani: "A Fair Balance" tra Interesse Generale e Tutela dei Diritti Fondamentali Individuali', in: A. Cannone *et al.* (eds.), *Studi in Onore di Vincenzo Starace*, 2008, vol. I, p. 745; see also Joint Opinion, *supra* note 191, p. 4.

210 The Treaty at a glance, *supra* note 69.