Data Protection in the European Union in Times of Terrorism

A Case Study on Passenger Name Record Agreements

Alba Bescos Pou

Abstract: The thesis is aimed at exploring whether the personal data of European citizens are protected under the counter-terrorism measures of the European Union from a legal perspective. Does an appropriate balance exist between security and data protection? What is the approach of the European Union? Does the EU provide a normative framework that ensures a high level of data protection? This thesis will determine the advantages and weaknesses of adopting a security or a data protection approach. Furthermore, it will show how the European Union has undertaken a human rights approach although some incoherencies and issues still remain. To that end the study closely analyses the European framework in the Area of Freedom, Security and Justice. Finally, a detailed analysis of the EU-US PNR agreement will be developed in order to underline the weaknesses of the European framework when it comes to undertaking particular measures which involve the exchange of information for law enforcement purposes.

Keywords: data protection, security, counter-terrorism, European Union, Passenger Name Record Agreements, Purpose limitation principle, proportionality, profiling.

I. Introduction

Different waves of terrorism have threatened our society over the last century. Multiple attacks have been perpetrated around the world. These attacks have been evolving over decades adopting new forms and using new tools and methods, which every year challenge counter-terrorism measures at national and international levels. Compared to colonial and authoritarian regimes, liberal democracies have not faced many extremely violent situations from revolutionary and separatists groups. However, they could not find a formula against terrorist attacks: in contrast, the opportunities provided by a free and democratic society, make the task of terrorist organizations and its operations much easier[1]. The effect of the globalization processes, for instance, the increased ease of movement not just within the same country, but also across borders, has been used by terrorist groups in the pursuit of destructive and lethal ends[2].

There is no doubt that the events that took place on 9/11 in New York and the subsequent attacks in London and Madrid promoted a change in the counter-terrorism policies in the United States and Europe. Those attacks became a threat to the peace and security of the international community and a fear of what will come next has spread among citizens of the different continents.

The European Union has recognised the interdependence between internal and external security and as a consequence the need to establish a "global security" strategy[3]. In that sense, the Resolution of the Security Council 1373 of 2001 calls on the international community to redouble its efforts to prevent and suppress terrorist acts and to strengthen international cooperation in response to such acts[4]. Since then, a series of interna-

[1] Paul Wilkinson, Terrorism versus Democracy: The Liberal State Response, (Frank Cass, 2006)20.
[2] Council of the European Union, Draft Internal Security Strategy for the European Union: "Towards a European Security Model", (2010)3.
[3] Trauner, Florian. Occasional Paper 'The Internal-external security Nexus: more coherence under Lisbon?', EU Institute For Security Studies, (2011)9.
[4] UNSC Res 1373 (2001) Paras 1-2.

tional legal measures at global, regional and bilateral level has been taken with the objective of cooperating in the prevention of activities such as aircraft hijacking, attacks on diplomats and hostage-taking, among others[5].

For fifty years the institutions and members of the European Union[6] have promoted and provided freedom and security, but the new methods used by terrorists has demonstrated the ineffectiveness of the security measures. For that reason the EU has strengthened its counter-terrorism policies to work towards the prevention of such attacks in the future.

There is no agreement on a definition on what "terrorism" is, but there is a consensus that terrorism includes a "strategy" whose objective is to create a climate of extreme fear[7]. Terrorist attacks are premeditated and planned. It is for that reason that the collaboration between intelligence agencies is necessary in order to develop and improve prevention mechanisms such as analytical tools or early-warning systems[8]. And it is at that prevention stage, when "personal data" becomes a key element in effective intelligence gathering. To have good results, all the necessary information should be available.

The European Union has been working on different agreements with third countries that directly affect the free movement of personal data of European citizens. Some examples are the EU-US Society for Worldwide Interbank Financial Telecommunication (SWIFT) Agreement or the Passenger Name Record (PNR) agreements. Those agreements have the same objectives: preventing, detecting, investigating and prosecuting terrorist offences and serious crime, based on an impact assessment[9]. For instance, the EU–US PNR Agreement, as its own text establishes aims to 'prevent and combat terrorism and serious transnational crime effectively as a means of protecting their respective democratic societies and common values'[10].

These new policies and agreements have a direct effect on the right to privacy of the citizens in Europe by allowing some practices that could entail a conflict with international and European standards in data protection. In the case of PNR Agreements, the EU argues that the information that will be shared is essential and that it cannot be obtained by other means. Following this line of argument, the PNR agreements constitute a necessary tool in the fight against terrorism[11].

But in any circumstance the personal data of any person deserves close protection from governmental intrusions, even when the government is dealing with national security concerns, due to its undoubtable link with individual dignity and personal freedom[12]. It is for that reason that it is important to evaluate if those measures that the European Union has undertaken respect the minimum standards on protection of personal data. Because, what happens when the measures that are supposed to protect our rights are at the same time violating them? The EU should work towards establishing a counter-terror strategy based on respect for human rights and fundamental freedoms[13] not because they are absolute, but because they represent the kind of democratic political values which its legitimacy is based on.

The diminished role of human rights is a result at least in part of the changing nature of security threats since 2001[14], and we cannot deny the difficulty that safeguarding security supposes whilst preserving the hu-

---

[5] Paul Wilkinson, Terrorism versus Democracy: The Liberal State Response, (Frank Cass, 2006)85.

[6] Council of the European Union, Draft Internal Security Strategy for the European Union: "Towards a European Security Model", (2010)1.

[7] Paul Wilkinson, Terrorism versus Democracy: The Liberal State Response, (Frank Cass, 2006)1.

[8] Council of the European Union, Draft Internal Security Strategy for the European Union: "Towards a European Security Model", (2010)12.

[9] Ibid.

[10] Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security. Doc No 17434/11 [2012] OJ L215/5 (EU-US PNR Agreement 2012).

[11] Ibid.

[12] Wilson R.A, ‚Human Rights in the War of Terror' in Wilson S.A (ed) *Human Rights in the ‚war of terror'*, (Cambridge University Press, 2005)27.

[13] Brower, Evelien, The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?, Centre for European Policy Studies, Working Document No. 320,(2009).

[14] Wilson R.A, ‚Human Rights in the War of Terror' in Wilson S.A (ed) Human Rights in the ‚war of terror', (Cambridge University Press, 2005)8.

man rights that are essential to democratic societies. But as Richard Ashby Wilson asked 'If we grant governments the authority to temporarily curtail certain liberties in emergency situations, how can we positively ensure that governments will not overstep the boundaries?'[15]

Sharing this concern, this thesis aims at analyzing the legal framework in the European Union on data protection in the light of counter-terrorism measures and the limits that human rights set on them. It is important to evaluate the current situation so as to be aware of the weaknesses of the current legislation.

This thesis will try to answer whether the personal data of European citizens is protected under the counter-terrorism measures of the European Union from a legal perspective.

In order to find an accurate answer, I will address as well the following questions: does an appropriate balance exist between security and data protection? What is the approach of the European Union? Does the EU provide a normative framework that ensures a high level of data protection? Far from willing to obtain just general statements, I will proceed to assay the Passenger Record Agreements Framework, with special attention to the EU-US PNR Agreement of 2011.

After defining the main concepts that the thesis will be dealing with: data protection, security and counter-terrorism, in Chapter II I will analyze how those concepts interact and the benefits and weaknesses of the different approaches that can be adopted by countries and international organizations while implementing measures in this area. This analysis will be mainly theoretical but some examples will be provided, with special reference to the European and the American policies.

In Chapter III I will analyze the position of the European Union concerning how to find a balance between its obligations of protecting personal data and ensuring the security of its citizens. For that purpose I will ascertain the legal framework of the EU on data protection and its limitations in terms of counter-terrorism. For that analysis, I will refer to the international legal background of this issue. Then, I will state if that regulation of the EU respects human rights standards, and in particular, if it is adjusted to the right to a private life from a legal point of view. In addition, I will try to state the position of the European Union in relation to the approaches mentioned in the first chapter.

In Chapter IV, I will focus on the Passenger Name Record Agreements normative framework. PNR is data provided by passengers when booking their flights that is collected by air carriers to handle ticket reservation. In those agreements between EU and non-European countries they require the air carriers operating in those territories to share the information about those passengers with the intelligence agencies of the countries concerned. This information is used as a tool in the prevention of and fight against terrorism and serious transnational crime. The PNR was included in the strategic objectives of the "EU Internal Security Strategy in Action" adopted in 2010[16]. In this thesis I will analyze the normative framework on PNR in the European Union, and to reinforce the analysis I will look closely at the EU – US PNR Agreement that came into force in July 2012.

Is the current regulation on sharing PNRs, and particularly the above-mentioned EU-US agreement, adequate in terms of the human rights standards that exist in the European Union? Is it a justified interference into the right to a private life? Are the Passenger Name Record Agreements adjusted to the European framework on data protection? What challenges remain in their regulation and implementation? In this chapter I will highlight how the human rights-based demands of proportionality, strict purpose limitation, the DHS duty ensure that the rights of access of the individual, rectification and erasure and the possibility of obtaining administrative and judicial redress and the limited usage of PNR data, among others, are fulfilled.

Finally, in Chapter V, I will present the conclusions as the answers to my research questions. As will be perceived throughout this research paper, the European Union, even if it is still far away from having a proper legal framework on the protection of personal data in what concerns security measures, in its willingness to fulfill with its international obligations, has been positively reformulating the legislation with the intention of obtaining a legal framework that puts human rights at the top of its counter-terrorism strategy.

---

[15] Wilson R.A, ‚Human Rights in the War of Terror' in Wilson S.A (ed) Human Rights in the ‚war of terror', (Cambridge University Press, 2005)10.

[16] Commission ´Communication to the European Parliament and The Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe', COM (2010) 673 final.

This analysis will be based on both primary sources (from the European Union and other relevant organizations, such as the OSCE), a study of the case-law of the Court of Justice of the European Union and the European Court of Human Rights, and a review of secondary sources, namely academic literature, articles and online sources. The thesis will use traditional legal methodology, but will encompass analyses from other sciences, such as the social sciences, when relevant.

During the evaluation we should keep in mind that although the EU must create a safe environment, in which its citizens can feel protected[17], a balance between security and freedom must be found. Most of the human rights, even when they are protected by the most important international treaties, such as the International Covenant on Civil and Political Rights, allowed states to limit their content for reasons of national security[18], but these interferences have to be proportional and necessary. To be able to find out what the proper balance is, we should underline that there is no such a thing as "zero risk". As Dwight D. Eisenhower said "If you want total security, go to prison. There you're fed, clothed, given medical care and so on. The only thing lacking…is freedom."

II. Data protection, Security and Counter-terrorism

In this second chapter the concepts of data protection, security and counter-terrorism will be delimited in sections A and B. Then, in section C, I will explain how these concepts are interrelated and the benefits and weaknesses of the approaches that the state can take in the trade-off between data protection and security. This analysis will answer the question whether there exists an appropriate balance between both elements in the area of counter-terrorism. In order to better illustrate the mentioned theoretical framework, a general overview of the United States and the European Union approach will be presented.

A. Data Protection as a Human Right

According to article 2 of the EU Data Protection Directive (95/46/EC) 'personal data means any information relating to an identified or identifiable natural person (data subject)'. Concerning that broad definition, we can include in it the concept of the so-called "ordinary personal data" which may include for instance name, address or number of passport of the data subject, but also "sensitive personal data", which includes ethnicity, religion, political affiliations, religion, etc.

What matters in this protection is who can process this information, by which means and to what end. Article 2 paragraph 'b' of the above mentioned Directive, defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collections, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'[19].

To determine who is controlling these data and who can have access to them, became an issue especially in the 1970s with the electronic revolution. Soon, with the normalization of the use of the computers and the arrival of the Internet, to determine who can be a legitimate data controller and the delimitation of the possibilities of acquiring, recording, using, consulting or deleting the personal data became a global concern. In response to this, the Organization for Economic Cooperation and Development (OECD) formulated, in 1980, the well-known OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data[20]. After those guidelines, some other regulations were developed at national, regional and international level.

[17] Council of the European Union, Draft Internal Security Strategy for the European Union: "Towards a European Security Model", (2010)4.

[18] See Art 4 of the International Covenant on Civil and Political Rights, 1966.

[19] Art 2 of the Directive 95/46/EC, of the European Parliament and of the Council, on the protection of individuals with regard of the processing of personal data and on the free movement of such data, [1995] OJ No L281/31. (Directive 95/46/EC).

[20] OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, 1980.

The protection of personal data becomes a necessity from the moment that these data contain information that concerns the private sphere of the data subject, and therefore has a direct link to the right to privacy protected in Article 12 of the Universal Declaration of Human Rights (UDHR), and in article 8 of the European Charter of Human Rights and Fundamental Freedoms (ECHR). The European Court of Human Rights (ECtHR) has underlined that the systematic collection and storage of personal information, falls within the scope of the right to a private life of the article 8 of the ECHR[21].

In what refers to the European Union, the European Charter of Fundamental Rights, just after mentioning the right to a private life of article 7, article 8 of the same charter foresees the protection of personal data as a right and establishes that these data should be protected and processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law[22].

What can be concluded is that the protection of personal data falls within the scope of human rights and fundamental freedoms already as an independent right in the case of Europe or included in the right to a private life. But in both cases, we should keep in mind that this is not an absolute right, which means that some necessary limitations in a democratic society can be imposed. Some of these limitations can be a consequence of the protection of the right to security[23] and the right of freedom of expression and information[24] of the others.

B. Security and Counter-Terrorism Measures

Security has been recognised as a human right in article 3 of the UDHR, and in article 9 (1) of the International Covenant on Civil and Political Rights, which states that "everyone has the right to liberty and security of person". Also Article 5 of the European Convention on Human Rights is concerned with the "right to liberty and security". Nevertheless, the concept of security in these texts has been usually reduced to a narrow definition essentially associated with liberty, which means that basically security is referred in terms of habeas corpus, torture, prisoner's rights, etc.

But it seems that a wider meaning was pursued by the legislator judging by the drafting process of Art.3 of the UDHR, where the drafting group rejected the use of other nomenclatures, such us 'physical and moral integrity' as it was considered included in the word "security"[25]. Following this rationale, for the purpose of this thesis, we will adopt a wider concept of security.

'Security' has different aspects, ranging from the traditional view of the international law of 'national security' to a more human rights based approach of 'security of the individual'. Being aware of the debate on the differences between the different approaches, we will consider 'human security' as the concept with the potential to reconcile the personal, national and international aspects[26].

Security is defined as the state of being free from danger or threat[27]. To guarantee a safe life for its citizens is considered, not just an obligation of the States under the article 9 of the International Covenant on Civil and Political rights and one of the main purposes for the international cooperation as the article 1 of the United Nations Charter states, but a necessary prerequisite to enjoying our civil liberties and other fundamental rights. It is for this reason that, the use of security reasons has been traditionally accepted as a legitimate argument to limit some of the people's rights, with the exception of the so-called absolute-rights such as the right to life or the prohibition of slavery. But at the same time, it is important to emphasise that we cannot ensure peace

[21] Amann v. Switzerland, App no 27798/95 (EctHR 16 February 2000)
[22] Art 8 of the Charter of Fundamental Rights of the European Union, 2010.
[23] Art 6 of the Charter of Fundamental Rights of the European Union, Art 3 UDHR and Art 5 ECHR.
[24] Art 11 of the Charter of Fundamental Rights of the European Union, Art 19 UDHR and Art 10 ECHR.
[25] Eide, Asbjorn, Alfredsson, Gudmundur, Melander, Göran, Rehof, Lars Adam, Rosas, Allan, Theresa, (eds) The Universal Declaration of Human Rights: A Commentary (Scandinavian University Press, 1992)77.
[26] Gerd Oberleitner, ´Human Security and Human Rights',European Training and Research Centre for Human Rights and Democracy (Occasioanl Paper Series, 2002)27.
[27] Online Oxford Dictionaries, <http://oxforddictionaries.com/>.

and security in a world where human rights are not respected[28]. In that sense, peace, justice, human rights and security are interlinked, and cannot exist without one other. As a consequence a balance should be found.

How to tackle the issue depends on which approach we adopt. We can understand that human security is achieved by strengthening the human rights framework and its implementation, or on the contrary we can interpret that we cannot ensure a respect for human rights if there is a lack of security in society. In this last approach, to be able to build a proper human rights system, first human security should be ensured.

As far as this thesis is concerned, of all the different threats that challenge the national security of the State, such as the lack of democracy, trafficking of human beings, hunger or social conflicts, we will focus on terrorism.

Despite all the efforts made in the international sphere, an agreement on what terrorism is does not exist. In general, the international community agrees that terrorism includes the following elements: a type of political violence, a tactic, involves fear beyond target, and the attacks are targeting non-combatant victims. There exists a variety of definitions of terrorism, not only at an international level, such as the one included in the UN Security Council Resolution 1566 (2004) or in the UN General Assembly Resolution 49/60 adopted in 1994 but as well at the European Union level, such as the one foreseen in Art.1 of the Framework Decision on Combating Terrorism (2002). This latter Decision states that, among others, 'shall be deemed to be terrorist offences: attacks upon a person's life which may cause death; attacks upon the physical integrity of a person; kidnapping or hostage taking; causing extensive destruction to a Government or public facility or seizure of aircraft, ships or other means of public or goods transport'.

Far from willing to start an analysis about the reasons that prevent the States from reaching an agreement, and to illustrate all definitions presented up to now, for the purpose of this thesis, and being conscious of its lack of precision, I will use the one contained in the International Convention for the Suppression of the Financing of Terrorism adopted in December 1999, which included the first general definition of terrorism in an International Treaty. According to the above-mentioned Convention, terrorism includes "any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act"[29].

Furthermore, it is important to distinguish between terrorism and organized crime, due to the fact that both concepts being used throughout the present thesis but not necessarily together. Once again, there is some discussion about the differences and links between both concepts, we simplify the debate by saying that organized crime usually looks for financial profit and tries to achieve as much control of the illegal market as possible. In contrast, terrorism, is motivated chiefly by ideological aims and pursues a political change[30].

The concept of counter-terrorism refers to the practices, tactics, techniques and strategies that governments, the military, police departments and corporations adopt in response to terrorist threats and/or acts, both real and imputed[31]. In that sense, we should emphasise the preventive mission of the counter-terrorism strategies. The main objective is to keep citizens safe from terrorists threats and attacks, and to ensure this safe environment, governments develop practices and techniques such as, the screening of airline passengers or the placing of video cameras in public places.

---

[28] Bertrand Ramcharan, *Human rights and human security: Strengthening Disarmament and Security (Disarmament Forum*, (UNIDIR/DF/2004/1) United Nations, January (2004)39.

[29] Art 2 of the International Convention for the Suppression of the Financing of Terrorism, 1996.

[30] Frank Bovenkerd and Bashir Abour Chakra, ‚Terrorism and Organized Crime', , in Schmid, Alex P. (ed) Forum on crime and society, Vol 4, No and 2,(New York: United Nations publications, 2004)3.

[31]US Foreign Policy About.com web site, <http://usforeignpolicy.about.com/od/defense/a/what-is-counterterrorism.htm>.

C. Trade-off between Data Protection and Security: the European Union and the United States approach.

Once the concepts of data protection, security and counter-terrorism have been delimited, in the following section I will explain, in the first subsection, how these terms are interrelated and the approaches that can be considered in the trade-off between data protection and security in the area of counter-terrorism measures. Then, the approaches of the United States of America and the European Union will be presented in subsections II and III.

1. Conceptual Issues

Among the challenges that nowadays face the international community, the fight against terrorism has been established as one of the priorities of the international community, as the UN Secretary General stated on his speech in New York, 22 January 2013, since acts of terrorism attack the most basic human rights, such as the right to life. But in establishing security measures to prevent possible future attacks, governments should avoid falling into the paradoxical situation whereby protecting the rights of their citizens they use measures that violate some of their other rights[32]. And as a consequence, we will inevitably find ourselves addressing the Hobbesian dilemma on "how do we defend liberty from imminent threats without compromising our hard-won freedoms"[33]. This is the question that has been challenging the policy makers for decades.

Counter-terrorism measures can affect several different types of rights. For instance, they can interfere with the prohibition of torture, freedom of movement, the right to a fair trial, freedom of thought, the presumption of innocence or, what more concerns us more in this study, privacy rights, including the protection of personal data.

It is true that to guarantee the security of their citizens, which as we have said before constitutes an obligation of the states, the interference with some of the rights mentioned above could hardly be avoided. But it does not mean that State can use any kind of measures to achieve security by denying human rights without complying with their obligations under international law. In other words, the states should respect the right to privacy of its citizens, even when national security issues are involved. As a consequence, they must work towards the enhancement of the protection of personal data, especially when these data are the object of counter-terrorism measures. The key to resolving this challenge is to find the appropriate balance or trade-off between data protection and security.

And just before studying this analysis in depth, it is important to highlight that as David Luban has stated, it is impossible to calculate how much truth there is in 'that the loss of our liberties makes us safer'[34]. The lack of exact empirical results is another reason why a previous discussion about the balance between values becomes a prime concern for this thesis.

Jennifer Chandler argues that security has a privileged position over other values, such as liberty. Even if that cannot be brought to an extreme where safety should be ensured at any price, there is still a belief in the general public that survival is basic precondition in order to be able to fully enjoy our civil liberties, including our right to privacy. To emphasise the obligation of the states to strengthen security measures Chandler refers to the theory of the social contract of Jean-Jacques Rousseau. As is well known, this theory holds that individuals have voluntarily consented to surrendering some of their individual freedoms and submit to a political authority in exchange for security and protection provided by the mentioned authority. For that reason, some

[32] Jennifer Chandler J, 'Privacy versus National Security, Clarifying the Trade-off', in Ian Kerr, Carole Lucock and Valerie Steeves (eds) Lessons From The Identity Trail: Anonymity, Privacy and Identity in a Networked Society (New York: Oxford University Press, February 2009)12.

[33] Wilson R.A, ‚Human Rights in the War of Terror' in Wilson S.A (ed) Human Rights in the ‚war of terror', (Cambridge University Press, 2005) 13.

[34] Wilson R.A, ‚Human Rights in the War of Terror' in Wilson S.A (ed) Human Rights in the ‚war of terror', (Cambridge University Press, 2005)26.

theorist can affirm that there is public agreement on the notion that security should be a priority for the governments, and that a subsequent restriction of individual rights can be legitimate[35].

Other scholars, such as Darren W. Davis or Brian D. Silver, state that another reason that drives people to opt for higher security even at the expense of their civil liberties is the existence of fear[36]. Terrorist attacks have taken different forms throughout the past few decades, but the unexpected severity of the attacks perpetrated on 9/11 in New York supposes a turning point. No one would ever have imagined that such dramatic acts were possible in a country with surveillance measures such as in the United States. As a consequence fear of what will be next has spread around our societies. This fear makes people expect a reaction from our governments. A reaction of the State towards strengthening the measures of control with the objective of keeping them safe, even if that means interfering with their privacy.

Moreover, we should keep in mind that as Peter Schieder explains, fear cannot be used as a political tool to reinforce the legitimacy of policy strategies[37]. Citizens have the right to demand protection, but letting fear blind our faith in our governments; can become a powerful instrument used for political purposes.

But despite all the arguments assuring that security should be at the centre of the policy making, we should remember the words of the United Nations High Commissioner for Human Rights in his Report in 2002, when he highlighted that 'to ensure that innocent people do not become the victims of counter-terrorism strategy should be an important component of anti-terrorist strategy'[38].

Furthermore, as Wolfgang Benedek states to spread fear, restrict fundamental freedoms and to make a change in security legislation, may be some of the objectives of terrorist groups in their attack against the strength of liberal democracies and push the system to failure[39]. For that reason, open societies should remain tied to their democratic values such as the rule of law, social justice, good governance and human rights, because these are the values most needed to keep our societies strong against those who try to destroy them.

Besides, the State cannot overlook its obligations under international law, in particular, under international human rights law. Specifically, the International Covenant on Civil and Political Rights (ICCPR) mandates the right to privacy, although the scope of its content is flexible enough to enable some restrictions, these ones must be necessary, legitimate and proportionate[40]. In that sense, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms in times of counter-terrorism, Martin Scheinin, in his report of December 2009, affirmed that even though the right to privacy is not an absolute right and that the State can legitimately limit it under international human rights law, 'every instance of interference needs to be subject to critical assessment'[41]. In other words, national security and counter-terrorism cannot be used as a simple argument to legitimatise limitations to the right to privacy or other civil liberties without going over a further check-list that should include principles such as necessity or proportionality.

In addition, most privacy intrusive measures are not always the most effective ones from the perspective of preventing terrorism[42]. It is important to keep in mind that human rights violations are considered a root cause

[35] Jennifer Chandler, 'Privacy versus National Security, Clarifying the Trade-off', in Ian Kerr, Carole Lucock and Valerie Steeves (eds) Lessons From The Identity Trail: Anonymity, Privacy and Identity in a Networked Society (New York: Oxford University Press, February 2009)126.

[36] Darren W. Davis, Brian D. Silver,. Civil Liberties vs. Security in the Context of the Terrorist Attacks on America Presentation at the Annual Meeting of the American Political Science Association (2002)5.

[37] Schieder, 2004, p.69.

[38] Yotopoulos-Marangopoulos A, ´Concluding Thoughts' in Benedek, Wolfgang and Yotopoulos-Marangopoulos, Alice (eds), Anti-Terrorist Measures and Human Rights. (Martinus Nijhoff Publishers, 2004)187.

[39] Benedek W, 'Human Security and Prevention of Terrorism' in Benedek W. and Yotopoulos-Marangopoulos A. (eds), Anti-Terrorist Measures and Human Rights (Martinus Nijhoff Publishers 2004)172.

[40]Martin Scheinin, Special Rapporteur on 'the promotion and protection of human rights and fundamental freedoms while counter terrorism', A/HRC/13/37 General Assembly, United Nations, (2009)7.

[41]Ibid 6.

[42] Ibid.

of International terrorism[43]. For that reason, human rights should be the central element of the antiterrorist strategy. As H.E. Jean De Ruyt had stated before the United Nations, on behalf of the European Union, 'integration of all countries into a fair world system of security prosperity and improved development is the condition for a strong sustainable community combating terrorism'[44]. In the same context, the EU Counter-Terrorism Coordinator, in 2012, stated that counter-terrorism measures that are unfair and discriminative, instead of achieving security, can create distrust and be a recruitment tool for terrorists[45].

Finally a third position in the trade-off between data protection and security can be adopted. I consider that a strong data protection framework does not mean upsetting the balance in favour of privacy, but it does mean keeping the perfect balance between both elements and we can ultimately deduce that the trade-off issue simply disappears. In fact, both elements, although they are sometimes incompatible, are at the same time complementary. As has been explained before, we need a secure society in order to ensure human rights, and we need to promote human rights in order to ensure security. Furthermore, high protection of personal data guarantees the obligations required by the right to privacy or right to data protection. At the same time, security will still be supported, because if the law enforcement authorities demonstrate that the use of certain data is necessary and proportional to prevent a threat to public safety, they will be able to use these data to the extent that it has been demonstrated to be necessary and proportional. Thus, nor even when data are processed by the public authorities would suppose to thrown off the balance in favour of security, because in this case the interference will be legitimate in the light of human rights. However, how to effectively prove that the use of data for security purposes is necessary and proportional still remains an issue.

Once a general framework on the trade-off between data protection and security has been outlined, in the following pages I will try to observe what is the approach of the United States` and the European Union's policies in that quandary.

2. The approach of the United States

The former President of the United States, George W. Bush, in his speech of November 6, 2001, assured that "No group or nations should mistake America´s intentions: We will not rest until terrorist groups of global research have been found, have been stopped, and have been defeated". This declaration of intentions marked the US approach in the trade-off between security and data protection although, as will be later explained, this trend changed under the presidency of Barack Obama. .

William Rehnquist, who was Chief Justice of the United States, in his book All the Laws but One: Civil Liberties in Wartime (1998), reformulating the two-thousand-year-old Roman maxim Inter arma silent leges ("In times of war, the laws are silent"), he expresses the American tendency to restrict civil liberties by stating that 'the laws will thus not be silent in time of war, but they will speak with a somewhat different voice'[46].

As in the European Union, the debate between civil liberties and national security in what concerns counter-terrorism measures have led to delicate discussions in the high government chambers of the United States and in particular between Republicans and Democrats[47]. It is true, that since the events of 9/11, American counter-terrorism strategy has been the target of criticism of human rights defenders. Special concern has been shown on issues related to detention conditions and domestic intelligence policies. These controversies highlight that,

[43] Christiane Bourloyannis-Vrailas, 'Human Rights as Standards and Framework Conditions for Anti-Terrorist Mesures' in Benedek, W, and Yotopoulos-Marangopoulos A, (eds), Anti-Terrorist Measures and Human Rights (Martinus Nijhoff Publishers, 2004)13-27.

[44] H.E. Jean De Ruyt, Permanent Representative of Belgium to the United Nations, on behalf of the European Union, 'Measures to eliminate international terrorism', (New York 1 October 2002)

[45] EU counter Terrorism Coordinator, 'EU Counter-Terrorism Strategy – Discussion paper', Council of The European Union, (2012).

[46] Wilson R.A, ‚Human Rights in the War of Terror' in Wilson S.A (ed) Human Rights in the ‚war of terror', (Cambridge University Press, 2005)8-9.

[47] Daniel B Prieto, 'Working Paper "War about Terror" Civil liberties and national security after 9/11' Council on Foreign Relations (2009)2.

at least, during the Bush administration, national security was considered a prime value even if that implied the sacrifice of some human rights.

In the matter of the protection of personal data, in general terms, we can state that American privacy policies have been taking a different direction from the European ones, mainly because the US sees the protection of these data as a consumer right in contrast to the European Union that considers it not just as a consumer right but as a fundamental right as well[48].

The United States uses a sectorial approach. There is no consolidated legal framework on protection of personal data. This perspective had led to the adoption of a long list of different laws concerning the treatment of data in different specific sectors. However the lack of a wider legal approach on this issue, leads to the existence of numerous loopholes[49].

Furthermore, partisans of privacy have had little success after the attacks of 11 September 2001. As Gehan Guneasekara explains, governments faced 'relatively little opposition' in adopting measures that under the pretext of the necessity of enhancing control had alarmingly restricted the existing privacy safeguards. A good example that illustrates this problematic situation is the adoption of the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act' (commonly known as the Patriot Act). This act reduces significantly the restrictions of the intelligence and counter-intelligence agencies in information sharing and expands the definition of terrorism, thus enabling an increase in the scope of its application[50]. The expansion of domestic intelligence programs has undermined civil liberties related to privacy, free speech and free association[51]. These measures undertaken by the United States represent a deterrent in the negotiations to adopt certain agreements with its transatlantic partner, the European Union. This is due to the fact that as contradistinction the EU has adopted a different perspective on the issue.

Notwithstanding these last statements, we cannot ignore the important progress that the US counter-terrorism strategy has made in the light of human rights, especially since the presidential elections in 2008. As Daniel B. Prieto emphasizes, there has been a positive evolution as a result of Supreme Court decisions, executive branch adjustment, and congressional action to moderate overreach and rectify errors[52]. Also, some District Courts had ruled that ‚the bulk collection of metadata by the NSA is in breach of the Fourth Amendment to the US Constitution'[53].

Another example, that reflects these improvements, can be found in the latest National Security Strategy of the United States published on May 26, 2010. The two previous ones, adopted in 2002 and 2006, under the Bush administration put their emphasis on the power of the American Army, and present the United States as a model democracy, legitimised to act and enforce its values abroad. In contrast, the last National Security Strategy issued by President Barack Obama uses a different tone in its composition, starting by choice of words such as "violent extremists" instead of the "terrorist and tyrants" used in the former strategies. Although the military is still underlined as an essential component of their national security and global leadership, the Strategy presents a more constructive approach. The President reminds us that the "strategy starts by recognizing that our strength and influence begins with the steps we take at home"[54]. Following this statement the strategy put its emphasis on the need to improve the economic situation and the protection of human rights and democratic values in the US, to be able to renew its leadership and be able to shape events abroad. Another element, with

[48] Susan Ariel Aaronson, Internet Governance or Internet Control? How to safeguard Internet Freedom, Cicero Fundation Great Debate Paper No. 13/01 (Gorge Washington University 2013)20.
[49] Ibid 23.
[50] Gunasekara, Gehan, 'The "Final" Privacy Frontier? Regulating Trans-Border Data Flows', International Journal of Law and Information Technology, Vol. 17 No.2, Oxford University Press, 2007. p. 159-162.
[51] Daniel B Prieto, 'Working Paper "War about Terror" Civil liberties and national security after 9/11' Council on Foreign Relations (2009)44.
[52] Ibid 3.
[53] European Parliament Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs 2013/2188 (INI), (2014)8.
[54] National Security Strategy, Washington, United States, (May 2010)3.

special relevance for this research, is that while the strategies signed under the Bush administration reminded silent on the subject, the Strategy of 2010 underlines the willingness of the State to balance the protection of civil liberties, including privacy, while pursuing national security[55].

Barack Obama represents, for some, the transformation of America. He had faced obstacles and scored some victories[56] for which he was awarded with the Nobel Peace Prize in 2009. However, and especially after the recent PRISM scandal[57] and public revelations in June 2013 of U.S. National Security Agency (NSA) surveillance programs, we should closely monitor the evolution of those changes, because as Gideon Rachman said in his article in the Financial Times, 'What is needed in Mr. Obama's second term is an America that is bolder in speaking out for human rights, political freedom and the protection of civilians – and more willing to make the point that these are universal principles that are not just applied when it is convenient'[58].

3. The Approach of the European Union

Once the United States approach has been presented, below I will focus on the European Union which, as we will see, differs from the first one.

The European Union has affirmed on more than one occasion that the counter-terrorism measures must be undertaken with 'full respect for human rights'[59]. As an example, Gilles de Kerchove, in his speech to the UN General Assembly as the European Counter-terrorism Coordinator, in September 2008, he stated that the third principle of the Union's counter-terrorism strategy is the concern with scrupulous respect for human rights and fundamental freedoms[60]. In fact, a few months earlier, Kerchove had affirmed that the position of the European Union was clear and in one direction: any measures undertaken to fight against terrorism should comply with obligations under international law, in particular with international human rights law. And in this same speech, he stated that 'Europeans have a long and, sometimes, difficult history of tackling terrorism. One important lesson we learned is that any shortcut around human rights makes you weaker'[61].

The EU is conscious that information gathering, sharing and analysis is the key factor in preventing and combating terrorism and other serious crimes, and to be effective, these measures should be carried out with the cooperation of third relevant parties, such as other non-member states or even some private companies, such as airlines. But in these processes, fundamental rights should be respected, in particular, the protection of personal data[62]. In that sense, we can affirm, that the European Union has adopted a human rights approach in the trade-off between security and data protection.

This can be reflected as well by the setting up of independent bodies that ensure that all the measures taken under the international organization competency, respect European standards on personal data. Those institutions, whose counterpart does not exist in the US, are the European Data Protection Supervisor (EDPS) and

---

[55] Ibid 37.

[56]The Biography Channel website, Barack Obama, 2013, http://www.biography.com/people/barack-obama-12782369.

[57] Savage, Charlie and Wyatt, Edward, 'U.S. Confirms that it Gathers Online Data Overseas', The New York Times, (6 June 2013.

[58]Rachman, Gideon, 'Obama should end his reticence on rights', Financial Times, (November 26, 2012) <http://www.ft.com/cms/s/0/1f80840e-37bc-11e2-a97e-00144feabdc0.html#axzz2OqJz1qdb> accessed 1 May 2013.

[59] Schorlemer S, 'Human Rights: Substantive and Institutional Implications of the War Against Terrorism' [2003] (Vol 14 No 2)278 European Journal of International Law (2003)278.

[60] Speech by the European Counter-Terrorism Coordinator, Gilles de KERCHOVE, to the United Nations General Assembly on the occasion of the Review of the UN Global Counter-Terrorism Strategy (New York, 4-5 September 2008) available at http://www.consilium.europa.eu/uedocs/cmsUpload/speechGANYengldef.pdf.

[61] Speech by Gilles de Kerchove, EU Counter terrorist coordinator - Prague, "Euro-Mediterranean Seminar: Counter-terrorism and human rights", 16-17 June 2008. Available at http://www.consilium.europa.eu/uedocs/cmsUpload/speech-Counter-terrorism_and_human_rights_GdK_june_08_rev.pdf.

[62] EU counter Terrorism Coordinator, 'EU Counter-Terrorism Strategy – Discussion paper', Council of The European Union, (2012)6.

the Article 29 Working Party on the protection of individuals with regard to the processing of personal data. In addition, in the area of Europe some instruments have been developed with the aim of adapting counter-terrorism to human rights standards, and of finding a balance between security and human rights, such as privacy and the protection of personal data. Some examples of this are the Guidelines on Human Rights and The Fight Against Terrorism of the Council of Europe, adopted on 11 July 2002 or the Practical Guidance Paper on Counter-Terrorism and Human rights developed by the Danish Institute on Human Rights, adopted in 2012 under the Danish Presidency of the European Union.

In fact, the difference between the approaches undertaken by the EU and the US recently became more evident after the 5th of June when The Guardian reported that the U.S. National Security Agency was using a national security electronic surveillance system (PRISM). In response to this, the Vice-President of the European Commission Viviane Reding, stated that '"the concept of national security does not mean that "anything goes": States do not enjoy an unlimited right of secret surveillance. In Europe, even in cases involving national security, every individual – irrespective of their nationality – can go to a Court, national or European, if they believe that their right to privacy or to data protection has been infringed. I have made my point clearly: this is what I want for European citizens also in the US'[63]. Here, we find a perfect example of the human rights approach undertaken by the EU, as opposed to the security approach adopted by the US.

However, even if in theory there is a clear human rights approach in the counter-terrorism strategy of the European Union, it would not be fair to ignore that, in practice, this has not always been achieved. An example is the former EU-US Passenger Record Agreement of 2004, which was open to criticism on several counts[64]. Even though that agreement was annulled by the European Court of Justice in 2006, the Court's ruling remains unclear whether the transfer of passenger data to the American Bureau of Customs and Border Protection would suppose a violation of personal data protection's regulations. In fact, the grounds for its decision lies elsewhere in that the agreement was taken based on the EU competences foreseen in the first pillar instead of the third one.[65]. In these shifting sands situations, we can observe the pressure that the United States approach brings on the European decision process. Moreover, the cooperation between the EU and US to combat terrorism, including police cooperation and intelligence sharing, has been established as a top priority, as Javier Solana established in New York, on May 2003[66]. That is why, the EU should beware of the negotiations with US in what concerns counter-terrorism policies, because, in the words of Gehan Gunasekara, 'In this sense the American security focus represents a very real 'Trojan Horse' for attacking the European privacy fortresses'[67]. For that reason, the EU should increase its efforts and review the transatlantic cooperation in intelligence-sharing, because, as the European Data Protection has established, the current situation has lead to a need to rebuild trust in global data flow in the aftermath of PRISM[68].

Also some issues remain in the area of the targeted restrictive sanctions (sometimes called ‚smart sanctions'). These sanctions involve asset freezing, travel ban, or arms embargo. Global terrorism has promoted the development of these measures, which initially had as a target third countries, and included non-state entities,

[63]European Commission web site http://ec.europa.eu/commission_2010-2014/reding/multimedia/news/2013/06/20130612_en.htm.

[64] Pring, Johnny, 'Up Close and Personal: Data Protection and EU-US relations", European Policy Centre (2007)2.

[65] C-317/04, Parliament v. Council [2006] ECR I-4795.

[66] Speech by Javier SOLANA, High Representative for the EU Common Foreign and Security Policy (CFSP) at the Annual Dinner of the Foreign Policy Association (FPA) on "Europe and America - Partners of Choice" (New York, May 2003).

[67] Gehan Gunasekara, 'The "Final" Privacy Frontier? Regulating Trans-Border Data Flows' International Journal of Law and Information Technology (Vol. 17 No.2, Oxford University Press, 2007) 162.

[68] European Union Press Release, ´Privacy and data protection can restore consumer confidence in the Digital Society' (Brussels 15 November 2013) EDPS/20013/11 <http://europa.eu/rapid/press-release_EDPS-13-10_en.htm> accessed 2 January 2013.

groups and individuals[69]. These sanctions by the EU are the result of the implementation of the UN Security Council Resolutions 1267 (1999), 1333 (2000) and 1390 (2002). Among the measures that those resolutions foresee, special interest relay in the obligation to take measures to freeze funds and other financial assets of individuals and entities associated with Osama Bin Laden, Al Qaeda and the Taliban. The individuals who should be targeted by these sanctions are designated by the Sanctions Committee, in a list which is continually updated.

While the EU member states are bound by SC resolutions adopted under Chapter VII, the EU it is not directly bound by them. It is however, obliged indirectly under Art. 48 (2) of the UN Charter. Since all EU states are members of the UN, they should promote the implementation of their obligations under the UNSC resolutions, in the area of the European Union when these obligations have implications with the competences of the Union[70]. But the application of those sanctions has led to some relevant case law, such as the Kadi case[71] decided by the European Court of Justice or the OMPI cases[72] ruled by the Court of First Instance. Some of the challenges the EU has faced are the implications that those sanctions have in relation to information sharing, procedural fairness (including accessibility and fair hearing) and effective remedy[73]. These issues illustrate how the European Union is concerned about the human rights implications in the area of counter-terrorism. However, when its competences are limited, such as in the area of targeted sanctions, the EU is being indirectly forced to respect the obligations of its members under the UN Charter, even when these may compromise the human rights protected under the Union.

However, it would not be fair to blame the weaknesses of the Human Rights Approach of the European Union to the US intelligence-gathering and other external institutions‘ practises. The Union, before undertaking any desicion or measure, should take a step back and remember for which values wants to stand for in order to defend a comprehensive approach to this sensitive issue.

D. Intermediate Conclusions

We can conclude by highlighting the difficulties that governments face in setting up a proper balance between privacy, data protection and security. States have to keep their citizens safe, but at the same time respect their privacy, as is foreseen in their obligations under international human rights law. These two values, as we have seen, are not always compatible. When such an incompatibility arises we should define our priorities: How much privacy we are ready to give up to guarantee our safety? Taking into account that it is not possible to keep ourselves safe from all the threats that attack our security, is the price that we pay at the expense of our civil liberties really worth the results that, as it has been said before, cannot be empirically demonstrated? These are the questions that will define the trade-off between privacy and security in what concerns counter-terrorism strategies.

Recalling the question posed at the beginning of this chapter about whether or not an appropriate balance between security and data protection exists, after this analysis we should give a negative answer, although to promote a strong framework with a high level of data protection has been proposed as a solution between both approaches. So far, neither the European Union nor the United States have demonstrated that they have the

---

[69] Mariani P, The Implementation of UN Security Council Resolutions Imposing Economic Sanctions in the EU/EC Legal System: Interpillar Issues and Judicial Review, Bocconi Legal Studies (Research Paper No. 1354568, Bocconi University – Department of Law, 2009)12.

[70] Ibid 3.

[71] Joined Cases C-402/05 and C-402/05, OJ 2008 C 285/2, Kadi and Al Barakaat International Foundation v Council and Commission, [2008] ECR I-000.

[72] Case T-228/02, Organisation des Modjahedines du Peuple d’Iran v Council [2006] ECR II-4665 ; Case T-256/07, People’s Mojahedin Organization of Iran v Council [2008] ECR II-03019; Case T-284/08, People’s Mojahedin Organization of Iran v Council, Judgment of 4 December 2008.

[73] For further information see Erika de Wet, *‘Human Rights Considerations and the Enforcement of Targeted Sanctions in Europe: The Emergence of Core Standards of Judicial Protection’, in Bardo Fassbender (ed) Securing Human Rights: Achievements and Challenges of the UN Security Council*, (Published to Oxford Scholarship Online, January 2012).

key to this issue, but over the past few years they have been working to at least get a bit closer to a proper solution. As we have seen throughout the last few pages, each approach has benefits and weaknesses. On one hand, to focus on strengthening the security of its citizens at the expense of their human rights might keep them safer, or at least in appearance, and might be appropriate to create the conditions for developing other rights. However, a policy focused on this security-centered approach, without taking into consideration other perspectives, can lead to a contradictory situation: while seeking to protect some rights, it can put in danger some other ones.

On the other hand, respecting human rights is an obligation of the state under international law, which has to be upheld. A human rights approach should also be considered since reaffirming the foundations and values of our open and democratic societies, is a victory against those who want to destroy them. Furthermore, if it is a fact that violations of human rights constitute a root cause of terrorism, then, would not putting an enhanced protection of human rights in the center of our counter-terrorism strategy be the logical consequence? Despite this last statement we cannot ignore that such an approach cannot be idealized. Data protection is a key element in an effective counter-terrorism strategy and to promote its exchange can be essential to prevent future attacks.

Then, the use of these data by the public authorities becomes essential to ensure security. In this context promoting safe movement of these data, and establishing a proper legal framework for their protection, is the key to understanding how to balance human rights and the fight against terrorism. In fact, as has been explained before, to ensure a strong framework with a high level of data protection would not only guarantee the obligations under the right to privacy, but at the same time would ensure security when the law enforcement authorities demonstrate that the use of these data is necessary and proportional. Thus, a third approach that considers enhancing the protection of personal data as a key issue in reducing the scope of the trade-off between both elements, or even making it disappear, can be put forward to resolve this dilemma.

For this reason, the following Chapter will set out the data protection legal framework for the purposes of counter-terrorism that exists in the European Union.

III. Legal Framework of the Protection of Personal Data applicable in the area of Counter-Terrorism of the European Union

In this chapter, the legal framework for the protection of personal data will be presented. I will not analyse all the existing legislation on data protection. I will focus on the part of it applicable to the Area of Freedom, Security and Justice (AFSJ) of the European Union since our concern is with the protection of data in the counter-terrorism measures undertaken by the EU, and the measures taken to combat crimes such as terrorism, are included in that area. Therefore, other areas, such as the protection of data for commercial proposes will not be treated in this thesis.

Before proceeding to an in-depth analysis of data protection regulation (section C) I will present the different legislative instruments existing at the moment and I will determine when each of them is applicable (Section B). But to understand the complexity and diversity of this framework we should bear in mind the so called 'three pillars' existing before the entry into force of the Lisbon Treaty in 2009, which will be explained in Section A. Finally, in Section D, I will highlight some of the challenges that still remain with regard to the protection of data in the AFSJ.

A. Background

The Treaty of Maastricht, in 1992, introduced an institutional structure that divided the areas of operation of the Union into three different pillars. The first[74] was the so called 'Community pillar' which referred to the three

[74]Wessel, Ramses A., 'The inside looking out: consistency and delimitation in EU external relations', Common Market Law Review [2000] (37: 1135 – 1171) Kluwer Law International, (2000)1135.

Communities: the European Community, the European Atomic Energy Community and the former European Coal and Steel Community. In addition, some other fields, such as the free movement of people were included in this first pillar after the Treaty of Amsterdam. The second pillar referred to the Common Foreign and Security Policy and the third one included police and judicial cooperation in criminal matters, to which relate most of the counter-terrorism measures.

Some examples of counter-terrorism measures based on police and judicial cooperation are the European Arrest Warrant, the Passenger Name Record Agreements, or the Visa Information System.

The entry into force of the Lisbon Treaty[75] established a horizontal approach abolishing the three pillar system. However, as we will see, some references to the former third pillar will have to be made in order to determine the current legislation applicable to the counter-terrorism measures undertaken by the Union.

Henceforth, and for the reasons that had been given above, I will only make reference to the data protection measures applicable to the Area of Freedom, Security and Justice, included in Title V of the Treaty on the Functioning of the European Union (the TFEU), which refers to the former third pillar, and some of the fields included in the former first pillar as well[76].

More explicitly, the area of Freedom, Security and justice aims to guarantee the free movement of persons and ensure a high level of security for European citizens. It covers different issues such as human trafficking, asylum, internal security, borders and visas, terrorism, organised crime and police cooperation[77].

B. Data Protection in the Area of Freedom, Security and Justice: applicable legislation

To explain the European data protection framework stricto sensu, it is important to underline in the first place the relevant international instruments in the area of Europe, that, despite the lack of binding effects on the European Union, have had a significant influence on that international organization.

1. Historical Evolution of the Data Protection Regime in Europe

First of all, it is necessary to mention the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[78], from September 1980, which contain a set of non-binding rules and principles that represented, by the time of its adoption, an international consensus on concern about the protection of personal information[79]. For that reason, those guidelines promoted the adoption of other international and regional mechanisms to tackle this issue.

Another international organization in the area of Europe, that is worth mentioning is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[80] of the Council of Europe from 1981 (hereinafter 1981 Convention), which came into force on 1 October 1985 for those who had ratified it. The 1981 Convention was the first international legally binding text. In fact, its ratification is also open to states non-members of the Council of Europe. This is the case, for instance of the recent ratification of the Treaty by Uruguay, in April 2013. This does not only prove its international relevance but as well the fact that despite being signed in the 1980s its content is still applicable nowadays. Furthermore, the drawing up of a new proposal is currently underway in order to modernize and overhaul the Convention[81].

---

[75] Alessadro Davoli. 'Personal Data Protection', Fact Sheets on the European Union, March 2011.

[76] European Union, http://europa.eu/legislation_summaries/glossary/freedom_security_justice_en.htm.

[77] European Union website http://europa.eu/legislation_summaries/justice_freedom_security/

[78] OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, 1980.

[79]The Organisation for Economic Co-operation and Development (OECD) http://www.oecd.org/sti/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldatabackground.htm

[80] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (1981).

[81] Council of Europe, http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp.

This document has had a significant influence on the European Union's policies. Although this text is not directly binding on the Union's legislator, the fact that all its member states have signed the mentioned Convention, makes if of interest for its members to promote the fulfillment of their obligations under the mentioned treaty. This includes what the competences that have been delegated to the EU. Therefore, despite the lack of binding effect on the EU, there does exist a link between the regulations adopted by the Council of Europe and the European Union. In fact, the EU has been using the 1981 Convention as a reference for the establishment of its own data protection normative framework. One example of this historical influence is the Convention based on Article K 3 of the Maastricht Treaty on European Union (from 1992) on the Establishment of a European Police Office (Europol Convention) adopted in 1995. Article 14 of the Europol Convention stated that the national legislation of its member states should ensure 'a standard of data protection which at least corresponds to the standard resulting from the implementation of the principles of the Council of Europe Convention of 28 January 1981'[82].

The 1981 Convention has the objective to protect personal data from potential abuses while they are collected and processed, and to regulate the cross-border flows of these data[83]. With regard to its content, it is important to underline Article 9 which allows derogations of some of the rights and duties contained in the Convention, if it constitutes a 'necessary measure in a democratic society in the interests of: a. protecting state security, public safety, the monetary interests of the State and of the suppression of criminal offences'.

In the context of the Council of Europe, and because of the influence that this organisation can have on the European Union, as has been explained above, the Council of Europe Guidelines on Human Rights and the Fight against Terrorism adopted on July 2002 are also worth mentioning. For the purpose of this thesis, and keeping in mind the lack of binding effects of this document, our interest lies in guideline V which refers to the 'Collection and processing of personal data by any competent authority in the field of State security'. It states that, in the context of the fight against terrorism, the interference into private life by the public authorities can be legitimate if the collection and processing of the personal data of the individual is governed by appropriate provisions of domestic law, it respects the principle of proportionality and is supervised by an external independent authority[84].

2. European Union Legal Framework

I will now explain the legislation and other instruments applicable in the area of the European Union, concerning data protection in the area of freedom, security and justice.

The entry into force of the Treaty of Lisbon provided some important changes in the protection of personal data. The first one is the fact that the mentioned Treaty gives binding force to the Charter of the Fundamental Rights of the European Union[85]. This has special relevance because since 2009 Articles 7 and 8 of the Charter, which foresee the right to a private life and the right to data protection and which provide minimum protection that should be foreseen in the future regulations have become legally binding on all member states.

The second and probably the most important change[86] of the Lisbon Treaty as far as this research is concerned is the inclusion of Article 16 of the TFEU. This article recognizes that individuals have the right to the protection of their personal data. It is important to underline that this article is included within the same Title as

[82] Convention based on Article K 3 of the (Maastricht) Treaty on European Union on the Establishment of a European Police Office (Europol Convention), [1995] OJ C316..

[83] Paul De Hert, Papakonstantinou V and Riehle C, ´Data Protection in the third pillar: cautious pessimism' in Maik Martind (ed), Crime, rights and the EU: the future of police and judicial cooperation (Publisher: Justice, February 2008)124.

[84] Guideline V of the Council of Europe, Guidelines on Human Rights and the Fight Against Terrorism, adopted by the Committee of Ministers. Strasburg: July 2002.

[85] Article 6 of the Lisbon Treaty amending the Treaty on the European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007.

[86]Hijmans H, 'Recent Developments in Data Protection at the European Union level', ERA - Europäische Rechtsakademie, (Published online, 2010)220.

other significant provisions such as consumer protection, environmental protection or the non-discrimination principle, which emphasizes the importance that the protection of data should receive.

Furthermore, the above-mentioned Article 16, in its second paragraph, imposes on the European Parliament and the Council the obligation to guarantee the protection of these data in all areas of action of the European Union. It is important to underline this new horizontal approach after the removal of the former three pillar system. Under the name of Title II, where Article 16 is included, this provision must have a general application. This obligation to protect the personal data should have wide scope, including the private and the public sector and all the institutions and bodies of the Union, even when they are acting within the areas included in the former third pillar. This provision pushed the Commission to launch a proposal for a new legal framework for the fundamental right to protection of personal data[87]. This proposal will be explained below.

Despite all that has been said, as Hielke Hijmans underlines, there are still some nuances in this new approach adopted under the Treaty of Lisbon. First of all, Article 16 of the TFEU is not applicable in the Common Foreign and Security Policy (the former second pillar). This has been the target of criticism, due to the fact that it had led to relevant problems. For instance, in relation to personal data processed in what are widely known as 'terrorist lists' and, as an example, the Kadi case already mentioned in the second Chapter[88]. The reason for its exclusion is foreseen in Declarations 20 and 21 attached to the Treaty of Lisbon. Those declarations state that in the application of Article 16 in relation to national security issues and in the area of judicial cooperation in criminal matters or police cooperation the 'specific nature of these fields' should be taken into account. It also foresees the possibility of establishing specific rules in those areas[89]. Thus, even theoretically Article 16 applies to the ASFJ, and although this area deals mainly with national security issues and police cooperation, everything seems to indicate that the law enforcement authorities would be able to justify the application of restrictions to the protection of personal data.

Finally, as a last nuance, the United Kingdom, Ireland and Denmark have circumscribed derogations on the Treaty of Lisbon in relation to the former third pillar[90]. These derogations in conjunction with what has been set out in by the two paragraphs above, emphasized that the allegedly abolished 'three pillar' system is still somehow present, and this reality remains the weakness of the new horizontal approach adopted in 2009.

To conclude the analysis of Article 16 of the TFEU, we should make a reference to the end of its second paragraph, where it states that 'compliance with these rules shall be subject to the control of independent authorities'. We can distinguish two main authorities whose main mandate is to monitor the application of the data protection legislation. Those institutions are the European Data Protection Supervisor and the Article 29 Working Party.

The European Data Protection Supervisor (EDPS) is an 'independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies'[91]. For that purpose, it monitors the EU administration during the processing of personal data and carries out advisory tasks on policies and legislation that affects privacy. Its competencies can be summarized as supervision, consultation and cooperation. The EDPS has published several opinions relevant to the content of this thesis. These

[87]European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protec-tion Regulation)', 2012/0011 (COD), COM(2012) 11 final. (COM (2012) 11 final)

[88] Hijmans, (n 86)221.

[89] Declarations 20 and 21 on Article 16 of the Treaty on the Functioning of the European Union, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, [2010] OJ 83/345.

[90] Hijmans, (n 86)221.

[91] European Data Protection Supervisor, http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en.

opinions deal with different issues such as the Passenger Name Record Agreements[92], EU Counter-terrorism policy[93] or information management in the area of freedom, security and justice[94].

The Article 29 Data Protection Working Party (hereinafter Article 29WP) was set up under Article 29 of Directive 95/46/EC of 24 October 1995. It is an independent advisory body that works for the protection of individuals with regard to the processing of personal data and on the free movement of such data[95]. Its competences are established in article 30 of the same Directive, which included, among other tasks, making recommendations, expressing opinions and drawing up an annual report. It is composed of the representatives of the supervisory authority of each member state of the EU, a representative of the authority established by the EU institutions and bodies, and a representative of the European Commission. Even though Directive 95/46/EC applies only to the former first and second pillars, in the past, the Article 29WP was very active, with its recommendations and opinions, with regard to the areas included in the third pillar[96].

Once the independent bodies that control the application of the core content of the right of data protection foreseen in Article 16 of the TFEU have been clarified, we should proceed to make a reference to the other current European measures applicable in this area.

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter DPD), is the main regulation on the protection of personal data in the European Union. This Directive foresees principles and guidelines, similar to the ones established by the OECD, to determine when the processing of data is lawful[97]. Nevertheless, this Directive cannot be applied in the area that we are dealing with.

Already in 2007, the European Court of Justice[98] ruled that the Directive was not applicable in the third pillar on Police and Judicial Co-operation in Criminal Matters (also named 'Justice and Home Affairs' or 'Area of Freedom, Security and Justice'). Currently, although the pillar system has been abolished by the Lisbon Treaty, this Directive is still not applicable because its Article 3 estates that the Directive does not apply 'in the course of an activity which falls outside the scope of Community law, such as operations concerning public security, defence or State security'[99]. Here we have an example where the former pillar system, is still, somehow, present in the Union. However, despite its legal exclusion, it is used as a reference in every area of the European law.

As regards the AFSJ there does not exist such a general regulatory framework. After 2001, different sectorial-specific norms were adopted, especially in relation to the EUROPOL, EUROJUST or the Schengen Information System (SIS). Among them it is important to underline the following ones: Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; the Council Decision 2009/371/JHA establishing the European Police Office; Council Decision 2002/187/JHA setting up EUROJUST with a view to reinforcing the fight against

[92] EDPS, Opinion of 25 March 2011 on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, [2011]OJ C 181/02.

[93] EDPS, Opinion of 24 November 2010 on on the Communication from the Commission to the European Parliament and the Council concerning the EU Counter-Terrorism Policy: main achievements and future challenges [2010] OJ C56/2.

[94] EDPS, Opinion of 30 September 2010 on the Communication from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice" [2010] OJ C355.

[95] European Union, http://ec.europa.eu/justice/data-protection/article-29/.

[96] Poullet Y and Gutwirth S, 'The contribution of the Article 29 Working Party to the construction of a harmonized European Data Protection System: an illustration of 'reflective governance'?' in Maria Veronica Perez Asinari & Pablo Palazzy (eds) Défis du droit à la protection de la vie privée. Challenges of privacy and data protection law (Bruylant, 2008)570 -610.

[97]European Union,
http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm.

[98] Joined Cases C-317/04 and C-318/04) Parliament v. Council, [2006] ECR I-4795.

[99] See Preamble Directive 95/46/EC, of the European Parliament and of the Council, on the protection of individuals with regard of the processing of personal data and on the free movement of such data, [1995] OJ No L281/31. (Directive 94/46/EC) para. 13 and 16.

serious crime, and Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences. Those regulatory norms establish specific norms for specific sectors.

Finally, due to concern about the lack of a general framework on data protection in the AFSJ, the Council Framework Decision 2008/977/JHA (hereinafter DPFD) was approved on 27 November 2008, on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. This decision was taken in order to enhance the protection of the data in the former third pillar[100]. It foresees the principles of lawfulness, proportionality and purpose, the right to be informed, the right to compensation in case of damage and, among other issues, it also list a set of minimum requirements to legitimise the transfer of data to competent authorities in third states or to international bodies[101].

It is true that the approval of the DPFD meant a positive step, but this Decision is still far from achieving the same level of protection as the DPD. Firstly, the Framework Decision is limited in its scope of application. It only applies to cross-border data processing, and not to the processing of data at national level[102]. Secondly, most of its provisions contemplate exceptions, which does not reflect a willingness to establish strong protection of personal data in the AFSJ. Finally, another aspect of the DPFD is the fact that, unlike the Directive of 1995, it does not establish the creation of any independent supervisory body to ensure a uniform implementation in the different member states[103].

Another important step taken in the area of our concern is the adoption of the Stockholm Programme by the European Council[104]. As is stated in its first section, this programme contains 'strategic guidelines for legislative and operational planning within the area of freedom, security and justice' in order to address the current challenges and improve the coherence between policy areas. This programme relies on the obligation foreseen under Article 68 of the TFEU, and has been adopted for the period 2010 – 2014.

This document refers to the protection of personal data in two different sections. The first one has as a title 'Protecting citizen's rights in the information society'. In that section the Council recalls the need for a comprehensive strategy to protect data within the Union, and also in what concerns the data sharing agreements between the EU and third countries, and especially with the United States. It also recalls in more than one paragraph, that the European regulation in this area should respect the principles set out in the 1981 Council of Europe Convention. And, among other suggestions, the Council invites the Commission to evaluate the current instruments on data protection and to present, if necessary new initiatives[105].

The second section in the Stockholm Programme that refers to data protection is entitled 'Managing the flow of information'. This section put its emphasis on the need to implement the 'Information Management Strategy for EU internal security'[106] which includes a strong data protection regime. It is important to underline as well, that the Council invites the Commission to set up a Union Passenger Name Record system, in order to ensure a high level of data protection, and based on an impact assessment.

Finally, one last instrument should be mentioned. The Commission, in line with the Council suggestions mentioned in the last paragraph, launched a Communication in relation to the 'Overview of information management in the area of freedom, security and justice' of 2010. This Communication set up a list of principles that should apply to EU instruments regulating the collection, storage or exchange of personal data for law

---

[100] See Preamble of the Council Framework Decision 2008/977/JHA, para.3.

[101] See Articles 3, 16, 19 and 13 of the Council Framework Decision 2008/977/JHA.

[102] Article 1 (4) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60. (Council Framework Decision 2008/977/JHA).

[103] European Parliament/ Legislative Observatory http://www.europarl.europa.eu/oeil/popups/summary.do?id=1188880&t=e&l=en (29 January 2014).

[104] European Council, The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens, Official Journal of the European Union, (2010).

[105] European Council, The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens, Official Journal of the European Union, Brussels, (2010)11.

[106] Council of the European Union, Draft Council Conclusions on an Information Management Strategy for EU internal security, Document 16637/09, Brussels, 25 November 2009.

enforcement or migration purposes[107]. For the purpose of determining the normative framework of the protection of personal data in the ASFJ, it is worth referring to each of those principles[108]:

b) Safeguarding fundamental rights. In particular the right to privacy and data protection of the Charter of Fundamental Rights of the European Union, even it also refers to article 16 of the TFEU. As well, in relation to this principle, the Commission calls for the application of the already explained 'privacy-by-design principle'.

b) Necessity. To justify the interference by the public authorities with the right of data protection, it should be necessary for national security, public safety or the prevention of crime.

c) Subsidiarity (as laid down in Article 5 of the Treaty on European Union) In order to use these instruments it is necessary to assess whether they achieve their objective, and whether regulating them at the EU level is more appropriate than leaving them in the hands of its Member States.

- *Accurate risk management*. In the elaboration of risks profiles, while using the personal data exchanged within those instruments, it is necessary to relay on evidence and not hypotheses.
- Cost-effectiveness. Due to the current economic situation, the cost of implementing the new instrument should not just be feasible and proportional but as well it should be proved that the same objective cannot be achieved using pre-existing instruments.
- *Bottom-up policy design*. In the development of new instruments, all the protagonists concerned should be consulted (including national authorities, financial bodies and civil society).
- *Clear allocation of responsibilities*. Instruments regulating the collection, storage or exchange of personal data for law enforcement or migration purposes, usually involve complicated IT structures and really complex implementation processes. For that reason, to identify who will be responsible for implementing and monitoring the instruments becomes an indispensable element in ensuring its success.
- *Review and sunset clause*. The proposals for new instruments in this area, should include, when possible, fixed periods for reviews, annual reports, and a sunset clause[109].

However even if those principles could be considered a positive step in adjusting the EU instruments to human rights standards, it is necessary to emphasise that a Communication is a 'policy document with no mandatory authority'[110]. In other words, it establishes political guidelines that should be followed by the member states but because it has no legal binging effects, there are no enforcement mechanisms if the authorities do not apply them.

We can conclude this second subsection by saying that the current Data Protection Framework within the Area of Freedom, Security and Justice of the Union is completely fragmented, and the need for new comprehensive legislation is becoming essential to for the fully respect the right to privacy and the right to data protection foreseen in the Charter of the Fundamental Rights of the European Union. On the one hand the DPFD which was meant to fulfil the need for this comprehensive approach is still far from guaranteeing an adequate level of protection. On the other hand, the Communication on the 'Overview of information management in the area of freedom, security and justice' issued by the Commission in 2010, does establish a set of principles in order to ensure coherence between EU instruments, but we should recall that a Communication is a politically binding instrument but it does not contain real legal obligations.

3. The Future of the European Union Legal Framework

This analysis would not be complete without mentioning two relevant processes that are taking place at the moment and that if they are successful in the near future, would bring significant changes in this area.

---

[107] European Commission 'Communication to the European Parliament and the Council, 'Overview of information manage-ment in the area of freedom, security and justice'', COM (2010)385 final. (COM(2010)385 final)4.
[108] Ibid 25.
[109] Ibid.
[110] European Commission website http://ec.europa.eu/civiljustice/glossary/glossary_en.htm (29 January 2014).

The first appeared as a consequence of the Stockholm Programme. As a response to the Council's invitation to evaluate the current instruments, the Commission adopted a legislative proposal on 25 January 2012, which includes a reform of the framework on the protection of personal data in existence at the moment[111]. This proposal has not yet been approved at the time of writing this thesis. In fact, the Commissions' will to obtain an agreement by May 2014 seems a little bit too optimistic, however there is stil hope that a consensus will be reached sometime this year, since last October 2013 the LIBE Committee adopted a decision on the opening of negotiations with the Council with a view to having the legal instruments adopted during this legislative term[112].

The Commission proposal foreseesa new comprehensive legal framework which will affect both, the private and public sector, including police and judicial cooperation. Apart from a General Data Protection Regulation on 'the protection of individuals with regard to the processing of personal data and on the free movement of such data'[113], it also launched a proposal for a Directive on the 'protection of individual with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data[114].

To understand why the Commission decided to elaborate two different proposals, one General Data Protection Regulation and one Directive in relation to the protection of data in the AFSJ it is necessary to briefly present the previous controversy about the form that this new data protection framework should have taken. In other words, if it would be better to update the Data Protection Directive and extend its scope to the area of police and judicial cooperation in criminal matters and afterwards develop the necessary sector-specific regulations or if it would be better to keep the current structure with the former third pillar remaining to be regulated in a completely independent norm[115].

On the one hand to gather the different existing regulations into a single norm seemed to be the most logical option to meet the need for a comprehensive approach and resolve the existing patchwork issue. The Commission seemed to be supporting this perspective as the Commissioner Viviane Reding confirmed in her speech in 2011[116]. Another reason to support the unification is the fact that the differentiation between the data processed by public or by private controllers is becoming difficult nowadays[117]. As in the example of the PNR the data that were once collected for commercial purposes are now used for security objectives. Thus, to differentiate the legislation applicable in each case can be dangerously confusing.

On the other hand, the special needs of the AFSJ, would lead to legislation with a great deal of specificities that would become difficult to understand[118]. Furthermore, Declarations 20 and 21 attached to the Treaty of Lisbon Treaty, in relation to Article 16 of the same Treaty, determine that the area of police and judicial cooperation has a specific nature which could require the need for specific rules in those areas. It is for the latter

---

[111] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protec-tion Regulation)', 2012/0011 (COD), COM(2012) 11 final; European Commission, 'Proposal for a Directive of the European Parliament and of the Council, on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free move-ment of such data', 2012/0010 (COD), COM (2012) 10 final.

[112] See the European Parliament Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs 2013/2188 (INI) (2004)15.

[113] COM(2012) 11 final, (n 111).

[114] COM(2012) 10 final, (n 111).

[115] Bigo, Didier; Carrera, Sergio; Gonzalez, Gloria; de Hert; Paul § others, Towards a New EU Legal Framework for Data Protection and Privacy, Directorate-General For Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs (ed) [2011] 98.

[116] Commissioner V. Reding, "Your data, your rights: Safeguarding your privacy in a connected world Privacy Platform "The Review of the EU Data Protection Framework", SPEECH/11/183, (Brussels, March 2011)3.

[117]Bigo, Didier; Carrera, Sergio; Gonzalez, Gloria; de Hert; Paul § others, Towards a New EU Legal Framework for Data Protection and Privacy, Directorate-General For Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs (ed) [2011]98.

[118] Ibid 104.

reasons, the Commission decided to elaborate two different legislative proposals as it is presented in their Explanatory Memorandum[119].

Because the mentioned proposal has not been approved at the time of writing this thesis its content will not be further developed. However, some references will be made to it in the following section.

The other process that is taking place at the moment, and which, at its conclusion, will have a significant influence on the area of data protection, even in the AFSJ, is the one that concerns the accession of the EU to the European Convention of Human Rights (ECHR).

The starting point of this process is Article 6 (2) of the Treaty on the European Union, in its consolidated version, which states that the Union 'shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms'. This accession, which is expected to take place in the near future, will have a significant impact including on the area of data protection[120]. I will not go into detail about the effects that this accession will produce, but it is worth mentioning some of the changes and challenges that the Union will have to face when the time comes:

- Article 276 TFEU states that the European Court of Justice 'has no jurisdiction to review the validity or proportionality of operations carried out by the police or other law enforcement services' in the area of common foreign and security policy. This limitation will not apply to the ECtHR, which will imply the possibility for the latter, to go deeper into the assessment of the treatment of data protection in this area[121].
- The ECHR does not contemplate the right to data protection as an independent right, as does the Charter of the European Union, but the ECtHR has stated in numerous cases that it is included within the scope of the right to privacy foreseen in Article 8 of the convention. Furthermore, the ECtHR has extensive case law on this issue, especially in applying the principle of necessity and the criteria of legitimacy of the processing, the purpose limitation principle[122] and, it has been active in the delimitation of concepts such as 'necessary in a democratic society', which have relevance in the AFSJ[123].

In this line of thinking we can conclude that the accession of the EU to the ECHR will inevitably bring relevant changes in the area of data protection with a clear inclination towards strengthening the protection of human rights.

Thus, in the light of the processes that have been explained, everything seems to indicate that eventually a new horizontal-comprehensive approach will finally take shape in the near future.

C. Remaining Challenges of the current Data Protection Framework within the European Union in the Area of Freedom, Security and Justice

Having presented the applicable legislation I will now identify the key challenges for protection of personal data in the AFSJ. I will focus on profiling and automated processing, the purpose limitation principle, the princi-

[119] See the last paragraph of the Explanatory Memorandum of the European Commission, 'Proposal for a Directive of the European Parliament and of the Council, on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free move-ment of such data', 2012/0010 (COD), COM (2012) 10 final.

[120] Bigo, Didier; Carrera, Sergio; Gonzalez, Gloria; de Hert; Paul § others, Towards a New EU Legal Framework for Data Protection and Privacy, Directorate-General For Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs (ed) [2011] 102.

[121] Polakiewicz J, ´EU law and the ECHR: Will EU accession to the European Convention on Human Rights square the circle?' (Oxford Brookes University, 2013)7.

[122] Perry v. UK, App no 63737/00, (EctHR 17 July 2003); P.G. & J.H. v. UK, App no 44787/98 (EctHR, 25 September 2001).

[123] Bigo, Didier; (n 120) 102.

ple of accountability, and the recent introduced concept of privacy-by-design. Although there are more challenges that we could analyse in this area, I will focus on this specific list so as to be able to provide a deeper analysis of each of them. One of these other issues concerning data protection in the area of AFSJ is the exchange of data with third non-members countries of the EU. This problematic issue will be further explained in the fourth chapter within the context of the Passenger Name Record Agreements.

For each of the challenges that will be explained below I will make reference to the Commission's proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, from January 2012, to determine if the proposed text would mark a turning point in this issue.

1. Profiling and automated processing

The increased use of personal data at an early stage and the necessity to prevent future terrorist acts or other acts derived from organised crime, have promoted the appearance of new techniques with the objective to identify potential suspects. This is the case in what we called security-related 'profiling', traditionally used for commercial purposes.

There is no one single definition of the term 'profiling'. The one adopted by the European Parliament understands that 'profiling' is 'the systematic association of sets of physical, behaviour or psychological characteristics with particular offences and their use as a basis for making law enforcement decisions'[124], originally adopted within the Opinion of the European Union Agency for Fundamental Rights of 28 October 2008 in the Proposal for a Council Framework Decision on the use of Passenger Name Record.

data for law enforcement purposes[125]. Some of the European regulatory norms do not refer to this issue under the name of profiling, but they do make reference to it using other kinds of nomenclatures such as 'automated individual decisions'.

It is also important to mention a concrete form of automated processing of data, namely 'ethnic profiling'. This technique bases the identification of suspects on their race, religion, political or philosophical beliefs or other sensitive data[126].

Profiles can be descriptive or predictive, and the latter is more problematic in the light of human rights. Descriptive profiles are the ones with the objective to identify those who have been involved in criminal acts, and the premises used for the profiling are based on evidence derived from the investigation of the act. On the other hand, predictive profiles are the ones with the objective to identify those suspects participating in a crime that will take place in the near future, or that has not been discovered yet[127]. Due to the fact that the second type of profiling is based on estimations, stereotypes and generalisations, and not on evidence, there is a high risk of obtaining the so called 'false positives' which involve innocent people becoming the object of arbitrary retentions, interrogations, visa refusals, placement on watchlists, and other measures that imply a clear interference into their right to privacy[128]. Furthermore, those incidents can promote a feeling of hostility and xenophobia towards certain groups of people.

---

[124] European Parliament, Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)). OJ C184E/119. Para C.

[125] European Union Agency for Fundamental, Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record data for law enforcement purposes, (2008)Para. 36.

[126] European Parliament, Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control [2008]OJ C184E/119 Para C.

[127] European Union Agency for Fundamental, Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record data for law enforcement purposes, (2008)Para. 36.

[128] European Parliament, Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control [2008] OJ C184E/119 Para I.

In this context, it is important to be aware that profiling techniques are not always more effective than random screening, as the security technologist Bruce Schneier remembers. Terrorists arrested till the hitherto come from Europe, Asia, Africa, the Middle East. They are male and female of different ages, different religions and pursuing different objectives[129]. It is for this reason that using generalisations and stereotypes is not an accurate enough method to determine certain criminal profiles and can easily bring policy makers into discriminatory paradigms.

With regard to the data protection framework of the EU, it is important to highlight that the DPFD of 2008 adopted a different position than the DPD in the matter of profiling techniques. The latter establishes a general prohibition and foresees the possibility of automated individual decisions as an exception[130]. The DPFD established a general authorisation but not without requiring two additional conditions[131]: the use of profiling should be necessary and pursue a legitimate interest[132].

The Commission's proposal from 2012, which, in the event of its being approved will replace the DPFD of 2008, adopts a general prohibition in its Article 9 of taking measures based on profiling and automated processing. It does foresee the possibility of using these techniques exceptionally when it has been 'authorised by law which also lays down measures to safeguard the data subject's legitimate interest'[133]. We can positively observe the fact that the proposal adopts the same direction as the DPD, and established a general prohibition of the use of profiling. Another positive step, is that in the second paragraph of the same article 9, it states that, in any case, the use of ethnic profiling, i.e. based solely on 'personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, genetic data or data concerning health or sex life', will be prohibited[134].

Profiling and automatic processing is a measure with a high risk of the individual being the object of discriminatory policies. For that reason, and due the lack of proven effectiveness, especially with regard to predictive profiles it is necessary to use it under limited circumstances, and when it has been proved to be necessary. Moreover, as the European Parliament already recommended to the Council, in April 2009, this measure should be implemented not only under the necessity requirement but also while fulfilling the proportionality principle.

Finally, among other recommendations of the European Parliament, it is important to underline as well, the need to ensure, an effective supervision by independent data protection authorities[135].

2. Purpose limitation principle

Purpose limitation is a core principle of the data protection framework in the European Union, as it was stated by the European Commission. It basically means that the data that has been collected for one purpose cannot be processed for other different purposes. However, some exceptions to this principle should be pointed out. This is the case of the SIS, SIS II and VIS. For instance the original purpose of the Visa Information System[136] (VIS) was to promote the cross-border exchange of visa data, but later its objective was extended to cover terrorism and other serious crimes prevention[137].

---

[129] Bruce Schneier, Profiling Makes Us Less Safe, Will profiling make a difference?, by The Editors, The New York Times, (2010) a<http://roomfordebate.blogs.nytimes.com/2010/01/04/will-profiling-make-a-difference/.>

[130] Art 15 Directive 95/46/EC.

[131] Art 7 Council Framework Decision 2008/977/JHA.

[132]De Hert P, and Bellanova R, Data Protection in the Area of Freedom, Security and Justice: a System Still To Be Fully Developed?, Policy Department C: Citizen's Rights and Constitutional Affairs, European Parliament, (2009)6.

[133] Article 9 of the COM(2012) 10 final.

[134] Articles 8 and 9 of the COM(2012) 10 final.

[135] European Parliament, Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)). OJ C184E/119 Para AC.

[136] VIS Regulation (EC) No 767/2008, Article 3.

[137]European Commission 'Communication to the European Parliament and the Council, 'Overview of information manage-ment in the area of freedom, security and justice'', COM (2010)385 final. 22.

The purpose limitation principle is contained not only in Directive 95/46/EC, but as well, in the DPFD, in its article 3 which states that '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'. Thus, this principle is applicable in the Area of Freedom, Security and Justice.

This principle has two parts: the data controller can collect data only for a determined specific purpose, and once data are collected they cannot be processed for other purposes different from the one for which they have been collected. This principle is of fundamental importance because in terms of the purpose set out for specific data, other principles linked to the quality of the data, such as adequacy, relevance, proportionality and period of retention will be determined[138].

Moreover, the definition included in Article 3 of the DPFD mentioned above, establishes that the purpose must be specific, explicit and legitimate. In other words it implies that the purpose should be expressed as clearly identifiable, unambiguously, and well enough defined in order to be able to set up sufficient and appropriate safeguards. Furthermore, the purpose should have a legal base and respect the non-discrimination principle, in order to be legitimate[139]. The determination of each measure's purpose according to the conditions explained above, is a prerequisite for other data quality requirements, and it contributes to transparency and legal certainty, delimiting how controllers are albe to use the personal data collected[140].

With regard to the new Commission's proposal of 2012, the text adopts the same perspective on this issue. Article 4 establishes the purpose limitation as a general principle of data protection. In particular it states that 'personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'.

As we can observe both, the proposal and the current DPFD, use nearly the same text as the DPD. For the purpose of this analysis it is important to underline the concept of 'incompatibility'. In April 2013, the Article 29 Working Party published an extensive Opinion[141] on the purpose limitation principle, and it makes special reference to what should be considered as a compatible use. Although the Opinion makes reference to the DPD and not to the DPFD, it sounds logical that those basic concepts should be understood in the same way in the entire data protection framework.

In this sense, the Article 29 Working party states that the limitation of incompatible purposes does not exclude the use of data already collected for other purposes different from the ones foreseen at the beginning[142]. But these new proposes should be accepted with some limits: they have to be specified, they must be legitimate, and they should fulfil all data quality requirements, such as necessity and proportionality[143]

As can be observed, this principle of purpose limitation can leave room for a wide range of exceptions.

In the AFSJ this purpose limitation remains a significantly challenge. Most of the personal data collected in this area is with the purpose of 'terrorism' and other 'serious crimes' prevention[144]. As has been set out in the Second Chapter of this research paper, agreement on what terrorism is does not exist. Furthermore, things become more complicated when referring to the concept of 'serious crimes', which is dangerously imprecise.

A clear example of this problematic issue is the VIS Regulation which in article 3 states that one of the purposes of the data collected will be 'to contribute to the prevention, detection or investigation of terrorist offences and of other serious criminal offences'. This Regulation was completed by the Council Framework Decision 2008/633/JHA, which in article 2(c) defines 'terrorist offences' as 'the offences under national law which correspond or are equivalent to the offences in Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13

[138] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13 (2013)4.
[139] Ibid 2.
[140] Stefano Tagliabue, the Working Party's Viewson Purpose Limitation and Big Data', International association of privacy professionals, August(2013).
[141] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13 (2013
[142] Ibid 12.
[143] Council Framework Decision 2008/977/JHA, Article 3 (2).
[144] Art 3 European Parliament and the Council, Regulation (EC) No 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), [2008] OJ 218/60.

June 2002 on combating terrorism. In addition article 2(d) defines 'serious criminal offences' as forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA' which refers to the European Arrest Warrant. Both definitions refer to their 'equivalent' in national law. Taking into account the existing differences and divergences among the national laws of the different Member States, a wide range of interpretations is provided on what we should understand as the purpose of the data collected under the VIS Regulation[145].

For those reasons, it seems doubtful that the VIS Regulation and other measures that make use of terms such as 'serious crimes' or 'serious criminal offences' as the purpose to collect personal data fulfil the specific and explicit purpose required in article 3 of the DPFD, unless a more accurate agreement on what those terms refer to comes into being.

3. Principle of Accountability

The increasing amount of personal data collected and the fast movement of these data due to the new technologies creates a reality where the control of the application of the data protection norms is becoming more and more difficult. Taking into consideration this situation the data controllers become the ones with most feasible means to control the protection of the individual's information. In this line of thinking, the principle of accountability pursues strengthening of responsibilities of the data controllers[146].

This principle it is not foreseen in the Directive 95/46/EC or in the Council Framework Decision 2008/977/JHA. This idea was promoted by the Article 29 Working Party, already in 2009[147] and one year later in their Opinion 3/2010 on the principle of accountability. Although both texts make reference to its implementation in the area of the Directive of 1995; it is not just possible but also necessary to apply this principle, in the AFSJ[148].

There is a need to attribute more obligations to data controllers to ensure that the principles and provisions contained in the data protection framework are being implemented. They should develop the necessary mechanisms, within their possibilities, to prove the compliance with the safeguards while data is being processed, to the data protection authorities or other interested parties, including, when necessary, the data subject[149].

Unlike the DPFD of 2008, the Commission's proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, even it does not use the same nomenclature, does adopt the idea of the principle of accountability, in article 18, under the heading 'Responsibility of the controller'. This article foresees in the first paragraph a general obligation of controllers to ensure that the processing of personal data fulfils the provisions adopted by the Directive. In the second paragraph it established a list of minimum obligations.

Thus, the assumption of the principle of accountability will reinforce the application of the provisions contained in the data protection framework, and will strengthen the transparency of the process.

---

[145] Bigo, Didier; Carrera, Sergio; Gonzalez, Gloria; de Hert; Paul § others, Towards a New EU Legal Framework for Data Protection and Privacy, Directorate-General For Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs (ed) [2011] 46.

[146]Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 00062/10 (2010)4.

[147] Article 29 Working Party, The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009.

[148] Bigo, Didier; (n 145) 111.

[149] Article 29 Working Party, The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, (2009)20.

4. Privacy-by-design

Directly linked with the accountability principle, there is the recent introduced privacy-by-design principle. Actually, based on the opinion of the EDPS, privacy-by-design is an element integrated in the accountability concept[150]. Furthermore, in the 32nd International Conference of Data Protection and Privacy Commissioners, in 2010, it was recognized as an 'essential component of the fundamental privacy protection'[151].

The concept of privacy-by-design appeared for the first time in Ontario, Canada, in the 1990s. It was developed by the Information and Privacy Commissioner, Dr. Ann Cavoukian, and soon attracted international attention[152].

Privacy-by-design pursues the integration of the data protection safeguards in the same information technologies and systems[153]. The idea is that taking into account that the data processing systems are neutral, it is true that their increasing number, use and interrelation can involve a risk for the protection of personal information, but it is also true that if the controllers design the systems in a way that the protection safeguards become an integrated part of them, they can also increase the control of the protection of these data. It does not mean adding some changes to the information systems afterwards but integrate them right from the beginning of its creation, in its original design. Thus, the protection adopts a proactive rather that a reactive approach, ensuring protection from the beginning of the process, when they are being collected, until the end of its use or existence, thereby, improving the transparency on the treatment of the personal data.

Furthermore, another added value is that the data subjects remain more protected, due to the fact that their privacy would be protected in an automatic way, without the need of any action on their part[154].

The adoption of this principle in the area of the European Union has been promoted[155] in recent years especially by the EDPS and the Article 29WP. It is true that this concept is not a completely new in the area of Europe in recent years. The DPD already makes a reference to this principle even though it does not refer to it as 'privacy-by-design'.

Article 17 of the mentioned Directive states that the controllers have the obligation to 'implement technical and organizational measures to protect personal data'. The EDPS and the Article 29WP have been lobbying for the introduction of the privacy-by-design principle, as such, in the future reform of the data protection framework, including in the AFSJ.

Current legislation, the DPFD, does not make reference to the principle of privacy-by-design. However, it seems that the efforts of the EDPS and the Article 29WP have had positive results. In fact, the Commission's proposal of 2012, introduced this principle in article 19, under the heading 'Data protection by design and by default'.

For the reasons that have been set out before and in line with the principle of accountability, if the proposal is adopted in the near future, the introduction of the privacy-by-design in the legal framework will ensure an

---

[150] European Data Protection Supervisor, Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union", OJ C 181/01, (2011)23.

[151] Resolution on Privacy by Design, adopted by the 32nd International Conference of Data Protection and Privacy Commissioners, (Jerusalem 27-29 October 2010).

[152] Information and Privacy Commissioner, Ontario, Canada http://www.ipc.on.ca/english/privacy/introduction-to-pbd/.

[153] Article 29 Working Party, The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, (2009)13.

[154] Ann Cavoukian, Information and Privacy Commissioner, Operationalizing Privacy By Design: A Guide to Implementing Strong Privacy Practices, (Ph.D, Canada: December 2012)12.

[155] European Data Protection Supervisor, Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union", OJ C 181/01, (2011) 23. And Article 29 Data Protection Working Party, The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data,(2009).20.

improvement in the implementation of the data protection provisions and it will, as well, provide a source of increasing the transparency of the processing.

D. Intermediate Conclusions

It is a fact that even though the Treaty of Lisbon foresees a horizontal and comprehensive approach of European policies, this is still not a reality as far as data protection in the area of freedom, security and justice is concerned. In contrast there is still a long way to go in order to achieve a legal framework with high protection of personal information of European citizens.

On the one hand the Council Framework Decision 2008/977/JHA has limited scope of application and as has been explained before, its provisions do not achieve the same level of protection as Directive 95/46/EC. However, everything seems to point out that the current reform of the data protection regulation and the accession of the EU to the European Convention of Human Rights will bring positive changes in this area in the matter of human rights.

Some of those positives changes have been explained in section C of this Chapter. Probably, the most positive change that the new proposal foresees is the adoption of the principles of accountability and the principle of privacy-by-design. Both, by amplifying the responsibilities of the data controller, one focusing on their daily tasks, and the other focusing on design of the data systems, adopt a proactive approach which will lead to an increase in the protection of data and provide the process with more transparency.

However, still some issues remain which have not really been solved in the Commission`s Proposal. For instance, regarding the purpose limitation principle, as has been explained before, the lack of concrete definitions of some terms such as 'terrorism' or serious crimes' can lead to a wider use of the EU instruments created to pursue these crimes.

Furthermore, the issue of profiling seems to be unresolved. The use of this technique is still possible and admissible according to the DPFD, although its use should be subject to requirements of proportionality and necessity. But its use is of high concern for human rights as has been explained above. Specially, in relation to predictive profiling, when the profiles are determined based on generalizations built upon prejudices.

The next Chapter will focus on a particular counter-terrorism measure based on the exchange of personal data, the Passenger Name Record Agreements.

IV. The Passenger Name Record Agreements

Having described in Chapter II, the trade-off between security and data protection and in Chapter III, the European legal framework in relation to the protection of personal information in the ASFJ, I will analyze how this policy and these principles apply in one specific counter terrorism measure of the European Union, the Passenger Name Record (PNR) Agreements. After explaining the concept (Section A), its background and historical evolution will be explained in Section B. Then, we will identify the legal framework applicable to this measure (Section C), and finally, the remaining challenges will be elaborated in Section D, with special attention to the EU-US PNR Agreement of 2011.

A. Concept

Passenger Name Record (PNR) data is the information that air carriers collect in their own database or in a database of another bigger computer reservation systems[156] at the time that passengers book tickets and at the time of the check-in on their flight. These records include information such as the name of the passenger, contact details, nationality, date and destination of the flight booked or the credit card details or other means of payment used[157].

[156] Bellanova, Rocco & Duez, Denis. A DifferentView on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage European Foreign Affairs Review 17, (Special Issue 109–124.© 2012 Kluwer Law International BV, 2012)115

[157] Bigo, Didier;(n 145)65.

It is necessary to distinguish between PNR data and Advance Passenger Information (API). API is used as an identity verification tool based on the information contained in the passenger's passport, i.e. name, place of residence, place of birth and nationality[158]. The API is regulated under the so called API Directive of 2004[159]. The member states of the EU hold these data for 24 hours for the purpose of improving border controls and combating illegal immigration[160]. In Article 5 of the same Directive, it states the possibility of using these data for law enforcement purposes, although this provision seems to be an exception more than a general purpose of the collection of the API data.

Some countries, in addition to requiring the transfer of API data, also oblige air carriers to transfer PNR data, which unlike the previous one, is being used mainly as a criminal intelligence tool in order to combat terrorism and other serious crimes[161].

The PNR data was initially collected for organizational and commercial purposes of the air carriers[162]. But it was after the 9/11 events, in 2001, that these data were conceived by the intelligence agencies as information of interest in order to fight terrorism and other serious crimes. In the aftermath of those attacks, the United States adopted legislation which imposed the obligation on the air carriers flying to and from American territory, to transfer the PNR data to the US Department of Homeland Security (DHS) under the threat of facing fines or even seeing denied the authorization to land on American soil, in case of a breach of that obligation[163].

The use of PNR data can be[164]:

- Re-active: the data is used within an investigation of a crime that has been already committed.
- Real time: the law enforcement authorities use the information provided by the air carriers in order to prevent a crime or retain one that is being committed at the moment of the processing the data. Unlike the re-active approach, in this case the suspects to be identified, are, in most cases, 'unknown'.
- Pro-active: the PNR data can be used as well for the creation of travel and behavior patterns, which can then be used for real time.

B. Background and Historical evolution of the use of PNR in the EU

As a response to the pressure exercised by the United States, and despite the internal disagreements within the same European Union institutions, in 2004 the first EU-US PNR agreement was signed, on the ground of the former first pillar. This was especially controversial due the EU regulation in relation to data transfers to non-member states. According to the DPD to do so the third country should guarantee that the data concerned would receive the same level of protection that these data receive within the Union[165]. This protection was not considered guaranteed in the US, or not at the same level as in the EU. An example is the Resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in Passenger Name Records transferred to the US Bureau of Customs and Border Protection[166], where the European Parliament states that the Undertakings appended for that Decision are not enough to ensure an adequate level of data protection. This problematic situation was not new. In fact in order to facilitate the exchange of information between Europe and the United States, they negotiated in 2000, the so called 'Safe Harbor Agreement', which enhanced the protection of data in the area of commercial purposes to what at the time was considered

[158] European Commission 'Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries', COM (2010) 492 final.4.
[159] Directive 2004/82/EC.
[160] Directive 2004/82/EC, Article 1.
[161] COM(2010) 492 final, (n 158)4.
[162] Bellanova,(n 156)114.
[163] Article 29 Data Protection Working Party, Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities, (2007)3.
[164] COM(2010) 492 final , (n 158)4.
[165] Chapter IV of the Directive 95/46/EC.
[166] European Parliament, Resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection, 22 March 2004.

as an acceptable level of protection. But as the Article 29WP has repeatedly underlined the provisions foreseen by this agreement are not enough[167].

In 2006, the CJEU annulled the EU-US PNR agreement, but its decision was based not on the lack of congruence with the DPD but on the Court's consideration that this agreement should have been undertaken on the grounds of the former third pillar instead of the first one[168].

That decision should not be seen as a triumph for data protection. On the contrary, to undertake agreements in the area of police and judicial cooperation in criminal matters meant that those measures fell out of the scope of the DPD and taking into consideration that the DPFD did not exist at the time, the personal information related to the transatlantic flights remained without any protection.

In the light of that situation an Interim EU-US PNR Agreement was undertaken in 2005, until a new Agreement was signed in October 2007[169].

In fact, over the past years the use of PNR data as a counterterrorism tool has increased around the world. Nowadays a relevant number of countries, such as New Zealand, Japan, South Korea, US, Canada[170] and Australia[171], are already using PNR for law enforcement purposes. So far, just the last three have signed an agreement with the EU[172]. Within the EU, the UK, France, Denmark, Sweden, the Netherlands and Belgium either already have a PNR system or are currently testing its use[173].

As we mentioned above, the EU regulation on data protection states that to allow a transfer of personal data to a third country, the latter should ensure the same level of protection as the one guaranteed in the Union. It is for that reason that the conclusion of those agreements with US, Australia and Canada have been the result of a long process, because each of them should ensure that the counterpart of the Agreement will protect the data of the passengers at European standards. In other words, to justify the adoption of those agreements, the Department of Homeland Security (DHS), the Canada Border Services Agency and the Australian Customs Service, who are the law enforcement authorities to whom the data is sent, have to assume the protection of the privacy of European citizens limiting the processing of their data to the terms established in the document of their Agreements with the EU.

On the other hand, the lack of a general European framework on the transfer of PNR data has resulted in each of those agreements having clauses that differ from the ones contained in the other agreements. For that reason, seeking to enhance the coherence of the EU law, the Commission launched a proposal in 2007 to regulate the collection, storing and analysis of PNR data for law enforcement purposes[174]. However, this proposal lapsed because of the entry into force of the Treaty of Lisbon.

After this period, some changes were implemented in the area of the European Union, which have been already mentioned in the previous chapter, and which had some influence on the protection of PNR data. Firstly, the adoption of the Council Framework Decision 2008/977/JHA. Secondly, the entry into force of the Lisbon Treaty, abolishing the former pillar system and introducing Article 16 of the TFEU, and finally, the publication of recommendations relating to the issues involving PNR agreements, such as the recommendation made by the European Parliament on the profiling issue[175], or Opinion 10/2011 on the proposal for a Directive of the Europe-

[167] Article 29 Working Party, Opinion 5/2012, p.17.
[168] See Judgment C-317/04 Parliament v. Council of the European Court of Justice, 30 My 2006.
[169] EU – US 2007 PNR Agreement.
[170] Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, 2006.
[171] 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, 2008.
[172] COM (2010) 492 final, (n 158)2 – 4.
[173] Ibid.
[174] European Commission 'Proposal for a Council Framework Decision, on the use of Passenger Name Record (PNR) for law enforcement purposes' COM (2007) 654 final.
[175] European Parliament, Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)). OJ C184E/119

an Parliament and the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime[176].

In the meantime, faced with the inexistent general framework on the transfer of PNR data, the Commission published a Communication in 2010 'On the global approach to transfer of PNR data to third countries'[177]. Even if a Communication has no binding effects, it tried to state some policy basis in order to provide some coherence for future agreements. This Communication will be further explained in the following section.

One year later, the European Commission, in response to the demand made by the European Council within the Stockholm Programme, decided to launch another proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for prevention, detention, investigation and prosecution of terrorist offences and serious crimes in February 2011[178]. This Proposal has not been approved at the moment of writing this thesis; in fact, on 24th of April 2013 it was rejected by the Civil Liberties Committee, by 30 votes to 25[179].

Furthermore, the European Union, in March 2011 started the negotiations[180] with the US in order to reach a general agreement on the protection of information while it is exchanged in the context of fighting crime and terrorism. This agreement will apply not only to PNR data, but also to any other exchange of information for law enforcement purposes. However, the EU-US Working Group on Data Protection which was set up in July 2013, at the time of writing this thesis an agreement has not yet been reached.

Finally, as a response to all these new emerging European norms, the European Parliament required the Commission to renegotiate the three PNR agreements existing at the time. As far as Canada is concerned, the negotiations are still taking place, and in the case of Australia, a new text has been agreed[181] although it has not been finally approved nor has entered into force so far. However, the new EU-US PNR Agreement[182] was finally approved by the European Parliament and the Council in April 2012, and entered into force the 1st of June 2012.

C. Legal Framework Appliable to the PNR Agreements

In order to identify the legal framework applicable to the PNR Agreements at the EU level, we can determine what are the existing regulations, laws and agreements in relation to PNR data nowadays. First there exist three PNR agreements which still apply at the moment, the EU-US one approved in 2012, the EU-Canada one in 2006 and the EU-Australia one in 2008.. The legal framework on which those agreements are based is formed by the DPFD. As has been explained before a specific European regulation on the transfer of PNR data has not yet been approved.

However the main applicable principles are mentioned in the non-binding strategy established by the Commission in 2010 in its Communication 'on the global approach to transfer of PNR data to third countries', as well

[176] Article 29 Working Party, Opinion 10/ 2011.
[177] COM (2010) 492 final (n 158)
[178] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes', COM (2011) 32 final.
[179] European Parliament News, 'Civil Liberties Committee rejects EU Passenger Name Record proposal', (2013) <http://www.europarl.europa.eu/news/en/pressroom/content/20130422IPR07523/> (29 January 2014).
[180] Official website of the Department of Homeland Security, United States and European Union Launch Formal Negotiations for an Agreement to Protect Personal Information Exchanged in the Context of Fighting Crime and Terrorism, 29 March 2011, <http://www.dhs.gov/news/2011/03/29/united-states-and-european-union-launch-formal-negotiations-agreement-protect.> (29 January 2014).
[181] Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, [2012] OJ L186/4.
[182] Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Brussels, Doc. No. 17434/11, [2012] OJ L215/5.

as in the Communication in relation to the 'Overview of information management in the area of freedom, security and justice' of 2010.

With regard to the DPFD some remarks should be made. This is the data protection regulation that applies to the PNR Agreements, due to the fact that 'the transfer of PNR data to the United States' Bureau of Customs and Border Protection constitutes processing operations concerning public security and the activities of the state in areas of criminal law'[183].It is for that reason, and in accordance with article 3 (2) of the DPD, that the PNR agreements fall outside of the scope of the DPD. As a consequence, the norm that applies in these cases is the DPFD.

Special attention should be paid to article 13 of the DPFD which refers to the transfer of personal data to third countries. This article states, in a similar way as do articles 13 and 25 of the DPD, that a transfer of personal data to a nonmember state of the European Union or to an international body will be legitimate 'only if it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and the transference is made to the competent authority'[184]. Furthermore, two other requirements must apply, but as has been criticized in Chapter II of this thesis, most of the articles included in the DPFD foresee an exception, and the two last requirements foreseen in article 13 are not exempt from this statement. The two last conditions required to legitimize a transference of personal data to a third country are:

- The Member State from which the data were obtained has given its consent to the transfer in compliance with its national law. This requirement does not apply if the transfer of the data is essential to prevent an immediate and serious threat to public security to any State or to 'essential interests of a Member State and the prior consent cannot be obtained in good time'[185]. Even though the last sentence of this paragraph imposes the obligation to inform 'without delay' to the authority that in the terms of the same article 13 should have given prior consent, the exception that this article 13.2 of the DPFD foresees is widely inaccurate. The use of imprecise concepts such as 'essential interests' or 'good time' can provide the law enforcement authority of the third country with the necessary tools to fit a wide range of exceptions to the requirement of obtaining the consent.
- The third State or international body concerned ensures an adequate level of protection for the intended data processing'. The level of protection should be evaluated[186] taking into account all the circumstances of the data transfer operation, the nature of the data, the purpose and the estimated duration of the pursued processing operations, the rules of law in force in the third State or the international body concerned and the professional rules and security measures which apply[187]. The third paragraph of the same article foresees derogation for this requirement, which raises some concerns. It states that the transfer of data to a third state will be legitimate even if the said state does not prove it has an adequate level of protection for the processing of the data concerned, when:
    - 'The national law of the Member State transferring the data so provides because of legitimate specific interests of the data subject; or legitimate prevailing interests, especially important public interests; or
    - The third State or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law'[188].

As regards the three PNR Agreements that the EU has signed so far, the Commission has taken a decision assessing the 'adequate protection' of the protection of the data before approving the mentioned agreements.

---

[183] C-317/04 Parliament v. Council [2006] OJ L82/15, 56.

[184] Council Framework Decision 2008/077/JHA, Article 13.

[185] Council Framework Decision 2008/077/JHA, Article 13.2.

[186] All the Commission decisions on the adequacy of the protection of personal data in third countries are available in the European Commission website, at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (29 January 2014).

[187] Council Framework Decision 2008/977/JHA, Article 13.4.

[188] Council Framework Decision 2008/977/JHA. Article 13.3.

In the case of Canada, the Commission published its decision 'on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency' on 6 September 2005. In the case of the US, the Commission determined the adequacy of the level of protection by the Department of Homeland Security, on 14th May 2004, on condition that the latter applies the obligations undertaken in the terms established in the Annex of the same decision[189]. However the European Parliament Draft Report, from January 2014, on ´the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs' states that as a result of the recent events, the United States does not guarantee an adequate level of protection of personal data of the european citizens according to european standards.[190]

Aside from these Decisions en relation to the adequacy of protection, other specific terms are included in the same PNR Agreements signed with the third country concerned.

For the purpose of defining the legal framework applicable, the Communication in relation to the 'Overview of information management in the area of freedom, security and justice' of 2010, should be mentioned. The content of this Communication has already been explained in the third chapter of this thesis, but for the purposes of this section, the set of principles foreseen in this document in relation to the EU instruments regulating the collection, storage or exchange of personal data for law enforcement or migration purposes[191], should be again underlined and related to the PNR systems.

Firstly, the PNR Agreement should respect the fundamental rights, including the right to privacy and data protection and apply the principle of privacy by design. Secondly, that the interference with those rights protected in the Charter of Fundamental Rights of the EU should be necessary for national security, public safety or prevention of crime. Thirdly, the EU should argue that a common regulation would be more effective than leaving it in the hands of its Member States. Fourthly, the elaboration of risk profiles should rely on evidence and not be hypothetical. Fifthly, taking into consideration the current economic situation, the cost of the PNR systems should be feasible and proportional and demonstrate that the same aims cannot be achieved using pre-existing instruments. Sixthly, the establishment of this system should take into account the opinion of all the affected parts, such as national authorities or civil society. Finally, a clear attribution of responsibilities and the inclusion of review and sunset clauses in the PNR agreements should be ensured.

Thus, all these principles should apply to the PNR Agreements signed by the EU. As we said before, the proposal by the Commission for a Directive on use of PNR data for the purposes of investigating serious crime and terrorist offences[192] has not been approved at the present moment, and as has been already argued in the last section, the closest to a European regulation on that issue is the Strategy established in the Communication[193] of the Commission in 2010 and the general provisions of the PNR.

The main objective of that Communication is to set up the basis for future PNR agreements between the EU and third countries[194]. The fact that each PNR agreement contains different clauses from the other agreements is inevitable, because the transference of the PNR should be adapted to the legal requirements and provisions foreseen in the third country concerned. But it does not avoid the fact that all of them should follow minimum criteria in order to ensure coherence in the strategy followed by the European Union. The content of this Com-

[189] 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 (notified under document number C(2004) 1914) (Text with EEA relevance) (2004/535/EC)

[190] European Parliament Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs 2013/2188 (INI), Jaunyary 2014, p.8.

[191] European Commission 'Communication to the European Parliament and the Council, 'Overview of information manage-ment in the area of freedom, security and justice'', COM (2010)385 final.25.

[192] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes', COM (2011) 32 final.

[193] COM (2010) 492 final (n 158)

[194] Ibid 3.

munication must be seen as minimum standards of protection, but the Commission enhances cooperation between parties in order to reach the highest level of protection in order to respect their obligation under human rights law.

To conclude , the transfer of PNR data to third countries has been established on a case to case basis. To determine the details of each regulation it will be necessary to refer to the Agreement signed by the EU with the third party. In the following section I will analyze the main issues on PNR agreements, and in order to illustrate them, I will focus on the one signed by the EU with the United States, which was approved in 2012 and will be valid until 2019.

D. The EU-US PNR Agreement: Challenges

Throughout the following pages I will analyze different issues that still remain in the PNR Agreements. To do so, I will specially focus on the following documents: The Communication from the Commission 'on the global approach to transfers of Passenger Name Record data to third countries of September 2010 (hereinafter Commission's Communication); the Opinion 7/2010 of the Article 29WP on the mentioned Communication; the Proposal for a Directive of the European Parliament and of the Council 'on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and desirous crimes' from February 2011, taking into account that this proposal has not been approved at the moment of writing this thesis, and the Opinion 20/2011 of the Article 29WP on the mentioned proposal. Finally, in order to exemplify that issue, I will determine how the last US-EU PNR Agreement from December 2011 approaches those challenges.

1. Necessity and Proportionality

The European Commission in its Communication to the European Parliament and the Council establishing an 'Overview of information management in the ASFJ', includes among the different principles that should apply to the instruments which include the collection and exchange of personal data, undertaken in the area of concern, the principle of necessity. For this reason the Commission recalls the jurisprudence of the European Court of Human Rights, which states that the interference with the right to data protection is justified 'if it is lawful, if it pursues a legitimate aim and if it is necessary in a democratic society'[195].

The first two requirements do not suppose a relevant concern, due to the fact that it is lawful as far as the measure is foreseen under EU law. Furthermore, there is no doubt that to try to achieve public safety is a legitimate aim. However, it is more complicated to assess the existence of the third requirement.

The ECtHR states that there will be necessity if the interference with the right to privacy, or more accurately, the right to data protection, answers a pressing social need, if the explanatory statement given by the public authority is relevant and sufficient, and if it is proportionate to the aim pursued[196].

Firstly, we should assess the existence of a social need which at the same time is linked with the existence of relevancy and sufficiency in the reasons given by the public authorities in the adoption of the PNR systems. It has been explained repeatedly throughout this research paper, that terrorism is a real threat for public safety nowadays and that the exchange of information between law enforcement authorities has a key role in establishing an efficient counterterrorism strategy. The same would apply to organized crime or other transnational serious crimes. However, it is necessary to recall the problematic issue set out in Chapter 3, in relation to what should be defined as serious crimes. Indubitably, a wider approach to those definitions will end up with the inclusion in some kind of crimes for which it would be more difficult to assess the existence of necessity of the interference with the right to data protection.

Secondly, it is more difficult to determine the proportionality of the PNR in relation to the aim pursued. It is necessary, at this point, to underline that PNR data is provided by the passengers, and subsequently, it should

[195] European Commission 'Communication to the European Parliament and the Council, 'Overview of information manage-ment in the area of freedom, security and justice'', COM (2010)385 final, 25.
[196] Ibid.

be qualified and treated as unverified information[197]. Furthermore, quoting the words used by the Article 29WP in its opinion 7/2010[198], the Commission in its Communication on the global approach to transfers of passenger information to third countries seems to point out that -'it is nice for the law enforcement authorities to have PNR data' rather than 'the law enforcement authorities need to have PNR data to combat terrorism and serious crimes'.

It it true that the use PNR data has been useful in achieving its purposes, for instance Belgium reported that '95% of all drugs seizures in 2009 were exclusively or predominantly due to the processing of PNR data'. Also Sweden reported that the high percentage (65-75%) of drugs seizures of 2009 was due to the processing of PNR[199]. Those statistics published in the Commission's proposal for a new PNR Directive should be read carefully. As a matter of fact, police authorities in order to render account of the use of personal information, and consequently, justify the accomplishment of their responsibilities, are self-interested in pushing those statistics up as high as possible. Furthermore, the text does not provide further details which seems suspicious, seeing that a better justification of these numbers would be beneficial in order to give higher credibility to the Commission.

In addition, those statistics only prove that the tool is effective, but they do not state if it would be able to achieve the same objectives with other existing systems such as the API or the VIS, and which would be a necessary element in determining the proportionality of these measures. This is the case, for instance, of the example used by the Directive on the use of PNR launched by the Commission in 2011, where it assures that PNR data is useful in identifying the most usual travel routes for trafficking people or drugs[200]. There is no reason to think that the same goal cannot be achieved by the use of API data.

However, it is also true that the previous mechanisms such as API, SIS or VIS are conceived as a border control rather than as an intelligence tool. They are mainly used to verify the identity of people at the border check -points. In this sense, those instruments are only effective for identification of suspects that are 'known'. Using r this argument, the Commission defends that PNR data are more appropriate to detect 'unknown' criminals or terrorists[201]. But even this counter argument supporting the use of PNR data cannot be easily brought down, it highlights the need to reduce the use of this personal information for what it is necessarily required and that cannot be achieved by any other means.

Additionally, to determine the proportionality in relation to the aim pursued, in other words, combating terrorism and serious crime, it should be guarantee that the exchange of data between law enforcement authorities be limited to the minimum necessary. This issue will be further discussed in the following subsection within the purpose limitation principle.

Finally, before ending the analysis of the 'necessity principle', one more issue should be addressed. The use of PNR data, as has been said before, involves an interference into the right to data protection, and it is because there is an interference that it should be foreseen as an exceptional measure. Consequently, any exceptional measure should be taken as far as the circumstances that had justified the necessity of its adoption prevail. Thus, there should be a temporary element. In this line of thinking, the Commission determines that those measures should include not just the possibility of periodic reviews, but as well a sunset clause[202]. The PNR Agreements that the EU has signed with Canada, Australia and United States foresee the obligation to review

[197] Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, 622/10 (2010) 5.
[198] Ibid 3.
[199] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes', COM (2011) 32 final, 6.
[200] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes', COM (2011) 32 final, 5.
[201] Ibid 7.
[202] European Commission 'Communication to the European Parliament and the Council, 'Overview of information manage-ment in the area of freedom, security and justice'', COM (2010)385 final, 27.

the implementation of those measures and as well a termination clause. In these terms we can state that there has been an improvement in the application of the principle of necessity, especially in the case of the EU-US PNR Agreement[203] from 2012, due to the fact that the previous one, approved in 2007 did not foresee a sunset clause.

2. Purpose Limitation.

As has been set out in Chapter III, the purpose limitation is a key consideration for most of the measures which consist of the exchange of data for law enforcement purposes within the European Union, including the PNR Agreements[204]. This principle states that the data that have been collected for one purpose cannot then be processed for other different purposes, even though some exception could apply. Moreover, this principle implies that the purpose should be explicit, clear and precise. As a consequence, the use of the data should not be wider than what is required in order to achieve the objective of the measure. For this reason the Commission's Communication on the global approach to transfer of PNR data to a third country, emphasises, that these data can only be used for law enforcement purposes in order to fight terrorism and other serious crimes[205]. At this point we should recall the problematic issue that was presented in the previous chapter about the lack of a precise definition of terrorism and serious crimes.

As far as the actual EU-US Agreement is concerned, it states that the PNR data will be processed for the purpose of preventing, detecting, investigating and prosecuting, terrorist offenses and related crimes, and other transnational crimes punishable with at least three years of imprisonment[206]. From a positive perspective it is necessary to underline that paragraph 1 of Article 4 of the mentioned Agreement, draws up a list of crimes that should be considered as included in its purpose, in a more exhaustive way than the previous Agreement of 2007. On the other hand, regarding the determination of 'other crimes that are punishable by a sentence of imprisonment of three years or more' it seems that in the last analysis the national criminal law will be the one that determines the crimes that will be persecuted while using PNR data. Here we can find a lack of precision which may easily lead to future disagreements.

Furthermore, in paragraphs 2 and 3 of the same article 4, it does foresee the possibility of using the data of the passengers in other kinds of situations or in the face t of other threats. Those statements are not foreseen as an exception, but as a real possibility, which seems to infer that nothing relevant has changed since 2004[207]. In other words that the purpose limitation principle is not being respected again in the new EU-US PNR Agreement not only because of its lack of precision but as well because of the open possibility of ending up with a wider purpose than the one strictly necessary to achieve the aim of this measure and to be able to qualify the interference of the right to data protection as justified.

In addition, in relation to the purpose of the PNR data, its pro-active use becomes an issue. As has been explained above, the passengers' data can be used for the creation of patterns, and it is in those processes that profiling becomes a challenge especially with regard to human rights. Thus, and in order to not repeat unnecessary information, I will limit myself to recalling the issue on profiling set out in the third chapter of this thesis, which can be considered applicable in relation to the PNR Agreements. In addition, it is necessary to underline that the EU PNR agreements include a prohibition of taking decisions with adverse effects for the individual only

[203] Article 23, 25 and 26EU-US PNR Agreement.
[204] European Commission 'Communication to the European Parliament and the Council, 'Overview of information manage-ment in the area of freedom, security and justice'', COM (2010)385 final, 3.
[205] COM (2010) 492 final. (n 158)8.
[206] Article 4of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Brussels, 8 December 2011. (EU-US PNR Agreement 2012).
[207] Hobbing P, ´Tracing Terrorists: the EU –Canada Agreement in PNR Matters' Centre for European Policy Studies Special Report (2008)41.

on the basis of automated decisions[208], in order to avoid illegal profiling. Even profiling still is an issue of concern especially in the cases where the law enforcement authorities process sensitive data as well.

The purpose limitation should not be understood only as the use of the data, but as well as the scope of the data. The latter should be kept to a minimum and in proportion to the aim to be achieved[209].

There is a clear tendency to consider that the use of sensitive data should be prohibited[210], because of the right to not be discriminated against for reasons such as sex, religion, political beliefs or ethnicity. However, the Commission's Communication foresees the possibility of using these data in exceptional circumstances where there is an 'imminent threat to loss of life and provided that the third country provides appropriate safeguards'[211].

Once again, the United States has been able to impose its will, and it managed to make use of this possibility to include, even in a really restricted way, the use of sensitive data in the new PNR Agreement. It does not just foresee the chance to process these data, if included in the PNR data, in exceptional circumstances, but as well it keeps the right to store these data for a period of 30 days, after which they will be deleted[212]. Here, the case of frequent travelers should be underlined, because in their case, this limited 30 days of retention after which the sensitive information should be deleted may not apply[213].

Despite the obligation by the DHS to mask this information immediately, and the duty to report it to the European Commission within a period of 90 days, it has not been justified as necessary and proportional to foresee any possibility of the use of sensitive data. In fact, one could argue that the use of these data would put on a limb the nondiscrimination clause included in the article 9 of the same agreement. However, this article does not make specific reference to the discriminative grounds that should be avoided, such as sex, race, color, ethnic or social origin, language, religion or belief, political or any other opinion, property, disability, age or sexual orientation. In contrast, the text just states that the 'Agreement apply to all passengers on an equal basis without unlawful discrimination'. To determine what the DHS understands by unlawful discrimination is a necessary issue that should be resolved and specified in order to ensure non-discriminatory treatment.

For this reason, it would be highly recommendable in the future agreement undertaken by the EU with third countries to impose the obligation that, in the case of any sensitive information about a passenger being sent to the authority of the third party, this information should be automatically deleted.

Apart from the issue of sensitive data, the PNR agreements include the transfer of certain information about the passenger. This information should be, as has been said before, strictly necessary. As the Commission's Communication suggests the PNR Agreements should include an exhaustive list of the data that would be object of the transfer. Following this suggestion, the EU US PNR Agreement[214], as well as the EU Australia PNR Agreement[215] does foresee a list with 19 items that should be collected and sent by the air carriers, which are really similar to the ones, foreseen by the Directive to regulate PNR at EU level proposed by the Commission. Taking as a reference the EU-US PNR Agreement, the items that the air carriers should transfer to the DHS are as follows:

- PNR record locator code

[208] Article 7 EU-US PNR Agreement 2012.

[209]European Commission 'Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries', COM (2010) 492 final,8.

[210] Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, 622/10 (2010) 6.

[211] COM (2010) 492 final, (n 209)8.

[212] Article 6 EU-US PNR Agreement 2012.

[213] Hornung, GErrit and Boehm, Franziska, 'Comparative study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record (PNR) to the United States Department of Homeland Security, Passau/Luxemburg, (2012)14.

[214] ANNEX EU-US PNR Agreement 2012.

[215] ANNEX 1 Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, [2012] OJ L186/4.

- Date of reservation/issue of ticket
- Date(s) of intended travel
- Name(s)
- Available frequent flier and benefit information (i.e. free tickets, upgrades, etc.)
- Other names on PNR, including number of travelers on PNR
- All available contact information (including originator information)
- All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)
- Travel itinerary specific PNR
- Travel agency/travel agent
- Code share information
- Split/divided information
- Travel status of passenger (including confirmations and check-in status)
- Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote
- All baggage information
- Seat information, including seat number
- General remarks including OSI (Optional Services instruction), SSI (Sensitive Security Information) and SSR (Special Service Requests information).
- Any collected API
- All historical changes to the PNR listed under points 1 to 8.

The Article 29 WP, in its Opinion 07/2010[216], underlines that the necessity and utility of each of those 19 elements have not yet been proved, and on some occasions it ensures that the API data should be enough to achieve the objectives expected. For that reason, although we cannot deny that the processing of passenger personal data for the purposes to fight terrorism and other serious crimes is useful, the necessity and the proportionality of the PNR agreements have not been stated, and consequently it is still not possible to ensure that we are dealing with a justified interference with the right to data protection.

3. Period of Retention and Storage

To retain the PNR data for a certain period is considered necessary as far as its re-active use is concerned, i.e. to enable the law enforcement authorities to investigate a crime that has been already committed it is necessary to allow them to use data collected in the past. The period during which personal data is collected and stored has a direct link with the proportionality principle that should apply to all EU instruments that involve the collection, storage or exchange of personal data for law enforcement purposes.

In the case of the PNR systems the Commission's communication states that the period of retention shall be no longer than that strictly necessary for the performance of the tasks to be conducted in order to achieve the purpose for which it was collected[217]. This restricted period should apply to all the law enforcement authorities that receive the PNR data.

But what is more disputed is the period of storage after the mentioned tasks are finalized. The Article 29WP is of the opinion that the data should be immediately deleted after this happens, unless a criminal investigation is open in relation to one specific passenger, or at least that no storage period should be allowed in the cases of

[216] Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, 622/10 (2010).4.
[217] European Commission 'Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries', COM (2010) 492 final,9.

non-suspect passengers, in other words, in the cases where the data of an individual did not appear as a match[218].

But it seems that the Commission and the European Parliament do not share the same opinion. In the Directive that the Commission proposed as a framework for the use of PNR in the area of the European Union, they state that the storage duration should be of 5 years[219], even if it also states that after 30 days the data should be masked. After this first short period these data would be able to be used only by limited authorized persons for the purpose of 'carrying out analysis of PNR data and developing assessment criteria'[220]. Basically, it means that all elements that could be used to identify the subject of the data should be hidden, for instance, the name or the address of the passenger.

There has been an evolution since the last proposal for a Council Framework Decision on PNR that the Commission launched on 2007, where it stated that the period should be of 13 years[221], and as well because after the short period of 30 days the data should be masked. However, although the reduction of the 13 year period to 5 years is a positive step in favor of data protection, it still has not been firmly argued that the 5 years period is a necessary and proportional one in order to fulfill the purpose of the PNR system. Furthermore, there is still the possibility of accessing to the full PNR data, even if that possibility is restricted, and the fact that the storage of data of passengers who are not suspects has not been proved to be proportionate to the aim pursued. For those reasons, if that Directive is approved, this issue will remain.

With regard to the EU-US PNR Agreement of 2012, the issue on the period of storage remains an issue of concern. Once data are received, it would take 6 months before the DHS would be obliged to mask and depersonalize the PNR data. Afterwards, a period of storage for up to five years is permitted. At the end of this period, data do not have to be deleted, rather, it is sent to a 'dormant database' where the data will be stored for a maximum of ten years for terrorist related crimes and five years for other kinds of crimes. The difference between this latter database and the previous one is that the access to data held in the 'dormant database' will be even more restricted than the one before, and will be only possible with special authorization, and the data will remain masked unless it is related to an identifiable case within a law enforcement operation[222].

As we can observe the Agreement foresees a long retention period for the personal data of the passengers, that despite all the restricted measures that may apply to access this information, it seems doubtful following the arguments presented by the Article 29 WP[223] that it can be argued as a proportional measure, and as a consequence, it becomes an unjustified interference with the right of data protection.

Furthermore, the fact that the other PNR Agreements that the EU signed with Canada[224] and Australia had considerably shorter periods of retention, i.e. 3.5 years in the first case, and 3.5 years plus 2 years in a dormant database in the second, leads us to think why should the US require such a long term, a total of 15 years, to achieve the same purposes.

---

[218] Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, 622/10 (2010) 6.

[219] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes', COM (2011) 32 final.8.

[220] Ibid.

[221] European Commission 'Proposal for a Council Framework Decision, on the use of Passenger Name Record (PNR) for law enforcement purposes' COM (2007) 654 final. Article 9.

[222] Article 8 of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Brussels, 8 December 2011. (EU-US PNR Agreement 2012).

[223] Article 29 Working Party, Opinion 10/2011.p. 6.

[224] European Commission 'Communication to the European Parliament and the Council, 'Overview of information manage-ment in the area of freedom, security and justice'', COM (2010)385 final, 18.

4. Method of Transmission

We can identify two methods of transmission of the personal information of the passengers from the air carriers to the law enforcement authorities of the third state which is the counterpart of the PNR agreement.

Firstly, there is the 'pull system' which is the method of data transfer for which the competent authorities have the possibility to access directly the air carriers database in order to take the PNR information which they are entitled to use.

Secondly, there is the so called 'push system' which is the method of data transfer by which the same air carriers filter the data that should be acknowledged by the law enforcement authorities. This information is collected, and the same air carrier sends it to the authorities.

It seems that the 'push system' is the one considered as the most acceptable in recent years. As an example, the proposal for a Council Framework Decision on the use of PNR for law enforcement purposes[225] made by the Commission in 2007, even if it stated a preference for the 'push system' offered the possibility of using both systems. In contrast, in the proposal made in 2011, it determined as the only possible method, the 'push system'. In fact, the Article 29WP qualified it as a more 'privacy friendly' method than the 'pull system'[226].

The EU-US PNR Agreement of 2012 adopted the same position[227]. Furthermore, as the Article 29 WP stated, it seems logical to attribute to the air carriers, as data controllers, the responsibility to filter all the information provided by the passengers at the time of booking a flight, and limit the transfer of information to the minimum required by the Agreement.

5. Data Subject's Rights

The Commission, in its Communication of 2010 states that every individual should have not only the right to access, rectification and deletion of their PNR data, but as well, he/she should have at his/her predisposition effective administrative and judicial redress procedures in case of a violation of his/her right to data protection. In addition, it underlines that in a case where the administrative or judicial authority determines that such a violation has taken place, the agreement should foresee effective sanctions and remedies to rectify the illegal situation[228]. Those rights are also foreseen by the Council Framework Decision 2008/977/JHA, in articles 17, 18 19 and 20.

The right of access seems to be regulated under Article 11 of the EU-US PNR Agreement of 2012. The first paragraph foresees the right of access to every individual without discrimination, but not surprisingly, in the second paragraph of the same article the United States retains the option to dismiss some of the information contained from accessing the subject's data if it is 'necessary to safeguard privacy-protected, national security, and law enforcement sensitive information'. Thus, the terms used in the Agreement are wide enough to provide the DHS with the means to apply the right of access under its own will.

Article 12 of the same Agreement foresees the right of the data subject to rectification and correction and deletion of the data. But, once again, in the third paragraph of article 12 it states that the US authorities could refuse the request of the individuals if that decision is justified under U.S. law.

In a similar composition, article 13 of the EU-US Agreement establishes the right to redress of the individuals, but this is regulated in accordance with US law. Thus, as Kristin Archick highlights, the effective exercise of the European citizens' rights will remain at the desire of the United States[229]. Article 13 makes reference to

[225] COM(2007) 654 final, (n 221).

[226]Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, 622/10 (2010) 6.

[227] Article 15 of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Brussels, 8 December 2011. (EU-US PNR Agreement 2010).

[228] European Commission 'Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries', COM (2010) 492 final.9.

[229] Kristin Archick, Kristin, U.S-EU Cooperating Against Terrorism, Congressional Research Service (2013)15.

some US laws which, in the opinion of the DHS entitle all individuals to exercise their rights and access and redress their information. However, just by way of example, the first law mentioned, the Freedom of Information Act (FOIA) gives the individuals the necessary means to access their information, but not to all of it. Thus, through the FOIA the individual has no right to know with which third parties his or her PNR has been shared[230]. Furthermore, the US has not been really effective in the recognition of those rights of access and redress to their own American citizens. This is the case for instance, of Hasbrouck v. U.S. Customs and Border Protection[231]. Thus, if US citizens are having problems making their rights effective, it seems worth pointing out that it would be even more difficult in the case of Europeans. In fact, this seems to be the real will of the DHS, especially with the inclusion of article 21 which states that the 'Agreement shall not create or confer, under US law, any right or benefit on any person or entity, private or public.'[232]

Individuals can think about enforcing their rights by using other means such as presenting an individual claim before the ECtHR against their own state, arguing that this state is not respecting their right to privacy foreseen in Article 8 of the ECHR. However, it is doubtful that this process would be effective, seeing that the consequence of a decision of the Court in favor of the individual would be to force the State to stop applying the European PNR Agreement. Ultimately, the victims will be, on the one hand, the air carriers who will face fines from the US government or even have to deal with a prohibition to land on US territory, and on the other hand, the same individuals who will see their possibilities of transatlantic movement restricted.

6. Supervision

As a final remark, we should determine the existence of the requirement mentioned in article 8 of the Charter of Fundamental rights, which in paragraph 3 establishes that the control of the protection of data should be carried out by an independent authority. What is more, this is required by the Commissions' Communication 'On the global approach to transfers of PNR data to third countries'[233].

It is a fact that the intelligence agencies share information in order to ensure our security, but who will determine that they are proceeding in the most respectful and least harmful possible way? Here it seems appropriate to recall the phrase 'Quis Custodiet ipsos custodies?' which literally translated means 'Who will guard the guards themselves?'[234].

In this sense, the new EU-US Agreement has been an improvement in relation to the previous ones, due to the fact that the new one introduces in article 14 the obligation to submit in compliance with the agreement to independent review and supervision. This supervision process should be carried out by the Department Privacy Officers such as the DHS Chief Privacy Officer. Thus, from a legal perspective a big step has been taken to ensure compliance of the terms of the agreements by the Parties. However, it must be mentioned that, critics have pointed out that a truly independent data protection authority in the US does not exist, or at least, not in relation to the standards required by the EU[235].

[230] Hornung, Gerrit and Boehm, Franziska, 'Comparative study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record (PNR) to the United States Department of Homeland Security, Passau/Luxemburg, 14 March 2012.18.

[231] Edward Hasbrouck v. U.S. Customs and Border Protection, United States District Court for the Northern District of California, San Francisco Division, order, No. 10-3793 RS.

[232] Article 21 EU-US PNR Agreement 2012.

[233] COM (2010) 492 final. (n 228)8.

[234] Dr. Bibi van Ginkel, 'Towards the intelligence use of intelligence: Quis Custodiet ipsos Custodes?', International Centre for Counter-Terrorism Research Paper (2012)1.

[235] Hornung, GErrit and Boehm, Franziska, 'Comparative study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record (PNR) to the United States Department of Homeland Security, Passau/Luxemburg, (2012)15.

E. Intermediate Conclusions

Throughout this fourth chapter I have presented the framework concerning the use of PNR data for law enforcement purposes, and I underlined the remaining issues in this area. Those issues are the assessment of necessity and proportionality, the purpose limitation principle, the period of retention and storage, the method of transmission and the protection of the data subject's rights.

The EU Commissioner for Home Affairs, Cecilia Malmström, affirmed that the new EU-US Agreement 'represents a big improvement over the existing Agreement from 2007'. However after analyzing some of the main challenges in the above subsection, there do not seem to be many changes, or at least, ones that are in favor of the protection of personal data. In fact the only improvements that this thesis has found is the establishment of the 'push system' as the only method of transfer of data, and leaving the 'pull system' for really exceptional circumstances, as well as the inclusion of the provisions related to the obligation of review and oversight. With regard to the other issues treated in this thesis, no improvement has been found. The new Agreement foresees the transfer of the same 19 items as the previous agreement, as well as the possibility of processing sensitive data. The purpose of its use is still quite broad and gives enough space to legally establish a wide range of exceptions during the implementation of the agreement.

Furthermore, the period of retention does not seem to have changed. Even if the new 'dormant databases' offer some more protection and guarantees than the active ones, the period is still too long to be considered proportional, especially if it is compared with the Agreements signed with Canada and Australia. Finally, and probably most importantly, it seems that the rights of the data subject are still far from offering the protection required by the Commission it its Communication of 2010[236] and the Council Framework Decision 2008/977/JHA.

Thus, it would be interesting to determine what the EU Commissioner for Home Affairs, Cecilia Malmström understands by the concept of 'big improvement'. In fact, it rather seems a poisoned apple in a new guise.

V. Conclusions.

The present study was designed to analyze the legal framework in the European Union on data protection in the light of counter-terrorism measures, in order to determine whether or not the personal data of European citizens are protected. This research has shown that although the EU, since 2001, has been active in developing a normative framework with a high level of data protection in the AFSJ, some issues still remain in terms of human rights such as the use of profiling activities.

In Chapter II the benefits and weaknesses of taking a security or a human rights approach has been explained. But, as that analysis underlines, whichever position the authorities take, it is really important to establish proper protection of personal data in times of counter-terrorism. On the one hand, data protection is a fundamental right protected under article 8 of the Charter of Fundamental Rights of the European Union. On the other hand, the use of this information by law enforcement authorities, as has been explained in detail above, plays a key role in order to ensure security. Thus, keeping a balance between privacy and security should guide the policy makers when it comes to establishing new strategies and counter-terrorism measures that involve the exchange of personal information.

As the concluding remarks in the second chapter have highlighted, so far, a formula to deal with this issue does not exist. The EU and the US have undertaken different approaches, but the lack of data about the efficiency and the outcome of their measures, prevent us from determining if the interference into the privacy of their citizens has been necessary and proportional. However, one thing is clear. If the exchange of information is fundamental in order to ensure security, then the establishment of a normative framework with a high level of protection of personal data in times of counter-terrorism is the key to keeping the balance between security and privacy rights. Furthermore, to promote a strong data protection framework does not just benefit privacy rights, but as well security issues, because if the law enforcement authorities demonstrate that the use of cer-

[236] European Commission 'Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries', COM (2010) 492 final, 9.

tain data is necessary and proportional in order to prevent a threat to public safety, then the interference will be still legitimate in terms of human rights.

In relation to the EU's approach, it has been shown that respect for human rights has been one of the aims of this regional organization, specially since the entry into force of the Treaty of Lisbon, when the Charter of Fundamental Rights of the EU became binding on all of its members. In addition, the incorporation of article 16 TFEU establishing a horizontal approach of the right to data protection, defined a new European approach in favor of human rights. However, since terrorism is an international concern for human security and cooperation with third countries has become a necessary tool in order to combat it, their policies have been challenged and political pressure has brought the EU to undertake measures which compromise the traditional European data protection framework. Thus, the Union is working in order to deal with the trade-off between security and data protection in all its areas of competence.

In Chapter III the data protection framework of the EU was presented. Even if there has been some criticism, it is important to underline the main remaining issues. This study has not been able to confirm that the protection of personal data reaches an adequate level of protection in the ASFJ, and in particular in relation to counter-terrorism policies.

Although Directive 95/46/EC provides high standards of protection, it does not apply in operations concerning public security, defense or State security. Thus the general framework applicable to the ASFJ relies on the Council Framework Decision 2998/977/JHA. However this Framework Decision has been highly criticized because it does not reach the same level of protection as the previously mentioned Directive. Furthermore, most of its provisions foresee situations where the law enforcement authorities will not be obliged to apply protection for personal data.

There have been some regulations developed in different specific sectors, such as in the area of the EUROPOL or the SIS, but the result of this approach has led to the existence of loopholes that have enabled the Union to take decisions that avoided protecting data according to European standards. To compensate this lack of regulation the Commission launched a Communication in 2010 on the 'Overview of information management in the area of freedom, security and justice'. As we observed, this Communication foresees a set of principles that should apply to the EU instruments that involve the exchange of personal information. Notwithstanding, a Communication does not have the same legal force as a Directive or a Council Framework Decision. Thus a stronger normative framework becomes, not just highly recommendable, but necessary.

Nevertheless, the Union has shown its willingness to achieve this goal and although the current situation is still far from being adequate in terms of human rights, it seems to be on the right path. As was developed in-depth before, the Commission has launched a Proposal for a Directive on the 'protection of the individual with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', which would contain a higher level of protection. It seems that this new proposal will bring positive responses to some of the issues that remain at the moment in this area, such as profiling and automated processing activities and the principle of accountability. In addition, the proposal foresees the insertion of some new principles, like the one related to the privacy-by-design, which will strengthen the level of protection of data of European's citizens. However, even if the proposal is approved in the near future, it seems that some issues will remain unsolved, for instance, that concerning the challenges of the application of the purpose limitation principle.

In fact, this latter issue should receive special attention. This principle is the one that justifies the processing of personal data and its exchange between law enforcement authorities in the area of ASFJ. The principle of purpose limitation is not only challenged because of the lack of accurate definitions of some terms such as 'terrorism' or 'serious crimes' but as well in relation to the scope of data, in other words, the type of data that is processed and exchanged. As an example of this problem, there is a general prohibition on using sensitive data even though some justifiable, exceptional cases can be accepted. An example of the use of this exceptional option is the EU-US PNR Agreement which foresees the possibility of processing these kinds of data for certain situations. It is for that reason that it is recommendable to take the delimitation of the use of personal

information as a primary concern when it comes to taking future measures in this area, not only because it is prescribed by law, but as also because the purpose of processing data has to justify the necessity of interference with the right of data protection.

Finally, in order to provide a more practical and concrete application of the issue of data protection within counter-terrorism measures, a closer analysis of the Passenger Name Record Agreements, has been developed in Chapter IV. Interference with the right to data protection that the PNR Agreements implied, and for the reasons explained within this fourth chapter, should be both necessary and proportional. The lack of a framework in this area has led to three agreements, signed with the US, Canada and Australia, which foresee different clauses and levels of data protection. It has been shown that the EU-US PNR Agreement does contemplate a level of protection that does not reach European standards. Furthermore, the differences between the agreements question the necessity and proportionality, if not of the measure itself, of the provisions which grant lower protection than that foreseen in other agreements. A good example of this is the periods of retention, which in the case of the US Agreement is disproportionally longer than the ones agreed with Australia and Canada.

Moreover, it is interesting to observe how the Agreement reached with the US is the one that has brought more concerns in terms of human rights. This leads us to think about how political pressure can redefine EU policies and how this fact can diminish the relevance of human rights within that organization. It is for this reason that in order to ensure the coherence of the Union's strategy and protect human rights in all its areas, including cooperation with third countries, there is a need to establish a proper legal framework. And in particular, with legal framework I mean a framework that should include norms with proper legal obligations, and not just political guidelines as in one of the Commission's Communications, which can be forgotten in the face of external political pressures.

In addition, after the entry into force of the Lisbon Treaty and as a consequence of the Stockholm Programme, three agreements that have been signed so far are being revised. This process has been already concluded in the case of the EU-US PNR Agreement, whose text was agreed on December 2011, and was finally approved by the Council in 2012, coming into force on July of the same year. In this study, relevant improvements in this new Agreement in relation to the former one from 2007 have not been found. There have been positive steps by establishing the 'push system' as the only method of transmission, and by including provisions in relation to the obligation of review and oversight. But some other challenges related to the purpose limitation principle, the scope of data, the prohibition of processing sensitive data, and the period of retention, are still of high concern in this new Agreement, in particular, from a privacy rights point of view.

Thus, the willingness of the EU to improve the protection of PNR data is questionable. As a consequence it will be interesting to observe whether the revision process that is taking place with Canada and Australia, will actually bring any improvement or if as in the case of the US, it will be old wine in new bottles.

Notwithstanding all that has been said and despite all the nuances of the European framework on data protection, during the last decade there has been a positive evolution. Furthermore, some new processes are taking place at the moment and which can bring about changes in order to strengthen privacy rights in this area. Some of these changes are the Commission's proposal for a reform of the data protection framework, which would involve the reform of the Directive of 1995 and the Council Framework Decision of 2008. Other processes are the Proposal for a Directive on the use of PNR data for the purposes of investigating serious crimes and terrorist offences[237], and the negotiations that started in March 2011, between the EU and the United States of America, so as to reach a general agreement on the protection of information within the context of counter-terrorism.

Thus, the data protection framework in relation to counter-terrorism measures found itself at one of the most dynamic moments so far in history, not only because of the new regulations that are being undertaken specially at EU level, but as well, because it is becoming a common concern of the international community as

[237] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes', COM (2011) 32 final.

has been prove by the international response to the PRISM scandal. Nevertheless, fresh analysis of the level of protection of personal information will have to be performed at the end of these processes in order to ascertain the outcome of these new regulations in terms of human rights.

In conclusion, and returning to the question posed at the beginning of this study, as to whether the personal data of European citizens is protected under the counter-terrorism measures of the European Union, this research has proved that although some protection is afforded we cannot yet affirm that the level of protection is adequate, for the reasons that have been put forward above and right through this thesis.

Alba Bescos Pou: abp12588@hotmail.com

Reference List

Monographies

Benedek W, 'Human Security and Prevention of Terrorism' in Benedek W. and Yotopoulos-Marangopoulos A. (eds), *Anti-Terrorist Measures and Human Rights* (Martinus Nijhoff Publishers 2004).

Bourloyannis-Vrailas C, 'Human Rights as Standards and Framework Conditions for Anti-Terrorist Mesures' in Benedek, W, and Yotopoulos-Marangopoulos A, (eds), *Anti-Terrorist Measures and Human Rights* (Martinus Nijhoff Publishers, 2004).

Chandler J, 'Privacy versus National Security, Clarifying the Trade-off', in Ian Kerr, Carole Lucock and Valerie Steeves (eds) *Lessons From The Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, February 2009).

Eide, Asbjorn, Alfredsson, Gudmundur, Melander, Göran, Rehof, Lars Adam, Rosas, Allan, Theresa, (eds) *The Universal Declaration of Human Rights: A Commentary* (Scandinavian University Press, 1992).

De Wet E, 'Human Rights Considerations and the Enforcement of Targeted Sanctions in Europe: The Emergence of Core Standards of Judicial Protection', in Bardo Fassbender (ed) *Securing Human Rights: Achievements and Challenges of the UN Security Council*, (Published to Oxford Scholarship Online, January 2012).

Frank B and Bashir Abour C, ΄Terrorism and Organized Crime', , in Schmid, Alex P. (ed) *Forum on crime and society*, Vol 4, No and 2,(New York: United Nations publications, 2004)**.**

De Hert P, Papakonstantinou V and Riehle C, ΄Data Protection in the third pillar: cautious pessimism' in Maik Martind (ed), *Crime, rights and the EU: the future of police and judicial cooperation* (Publisher: Justice, February 2008).

Poullet Y and Gutwirth S, 'The contribution of the Article 29 Working Party to the construction of a harmonized European Data Protection System: an illustration of 'reflective governance'?' in Maria Veronica Perez Asinari & Pablo Palazzy (eds) *Défis du droit à la protection de la vie privée. Challenges of privacy and data protection law (*Bruylant, 2008).

Ramcharan B, *Human rights and human security: Strengthening Disarmament and Security* (Disarmament Forum, (UNIDIR/DF/2004/1) United Nations, January 2004).

Schieder P, ΄Anti-Terrorist measures and Human Rights from the Prespective of teh parlyament of the Council of Europe' in Benedek, Wolfgang and Yotopoulos-Marangopoulos, Alice (eds), *Anti-Terrorist Measures and Human Rights* (Martinus Nijhoff Publishers, 2004).

Wilkinson, P, *Terrorism versus Democracy: The Liberal State Response* (Second Edition, Frank Cass, 2006).

Wilson, R.A, ΄Human rights in the 'War on Terror'',In Wilson, R.A. (ed), *Human Rights in the 'War on Terror'*, (Cambridge University Press, 2005).

Yotopoulos-Marangopoulos A, ΄Concluding Thoughts' in Benedek, Wolfgang and Yotopoulos-Marangopoulos, Alice (eds), *Anti-Terrorist Measures and Human Rights*. (Martinus Nijhoff Publishers, 2004).

Articles

Alessadro Davoli. *Personal Data Protection'*, Fact Sheets on the European Union, March 2011.

Ann Cavoukian, *Information and Privacy Commissioner, Operationalizing Privacy By Design: A Guide to Implementing Strong Privacy Practices,* (Ph.D, Canada: December 2012)

<http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf> Accessed 1 January 2014.

Bellanova, Rocco & Duez, Denis. *A DifferentView on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage* European Foreign Affairs Review 17, (Special Issue 109–124.© 2012 Kluwer Law International BV, 2012)

Bigo, Didier; Carrera, Sergio; Gonzalez, Gloria; de Hert; Paul & others, Towards a New EU Legal Framework for Data Protection and Privacy, Directorate-General For Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs (ed) [2011] < www.ceps.eu/ceps/dld/6351/pdf> Accessed 1 January 2014.

Brower, Evelien, *The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?,* (2009) Centre for European Policy Studies, Working Document No. 320 < Brower, Evelien, The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?, Centre for European Policy Studies, Working Document No. 320, 2009> accessed 12 Desember 2013.

DW., Davis Silver B D. *Civil Liberties vs. Security in the Context of the Terrorist Attacks on America* Presentation at the Annual Meeting of the American Political Science Association (2002)
<http://www.apsanet.org/~polcomm/news/2003/terrorism/papers/davis-silver.pdf> Accessed 1 Desember 2013.

De Hert P, and Bellanova R, *Data Protection in the Area of Freedom, Security and Justice: a System Still To Be Fully Developed?*, Policy Department C: Citizen's Rights and Constitutional Affairs, European Parliament, (2009).

Dr. Bibi van Ginkel, '*Towards the intelligence use of intelligence: Quis Custodiet ipsos Custodes?*', International Centre for Counter-Terrorism Research Paper (2012) <http://www.icct.nl/download/file/ICCT-van-Ginkel-Intelligent-Use-of-Intelligence-August-2012.pdf> Accessed 15 October 2013.

Gunasekara G, 'The "Final" Privacy Frontier? Regulating Trans-Border Data Flows' International Journal of Law and Information Technology (Vol. 17 No.2, Oxford University Press, 2007) 159-162.

Hijmans H, 'Recent Developments in Data Protection at the European Union level', ERA - Europäische Rechtsakademie, (Published online, 2010).

Hobbing P, ´Tracing Terrorists: the EU –Canada Agreement in PNR Matters' Centre for European Policy Studies Special Report (2008) < http://aei.pitt.edu/11745/> Accessed 1 September 2013.

Hornung, GErrit and Boehm, Franziska, 'Comparative study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record (PNR) to the United States Department of Homeland Security, Passau/Luxemburg, 14 March 2012.

Kristin Archick, Kristin, U.S-EU Cooperating Against Terrorism, Congressional Research Service (2013) <http://www.fas.org/sgp/crs/row/RS22030.pdf> Accessed 1 September 2013.

Mariani P, The Implementation of UN Security Council Resolutions Imposing Economic Sanctions in the EU/EC Legal System: Interpillar Issues and Judicial Review, Bocconi Legal Studies (Research Paper No. 1354568, Bocconi University – Department of Law, 2009).

Oberleitner G, ´Human Security and Human Rights',European Training and Research Centre for Human Rights and Democracy (Occasioanl Paper Series, 2002).

Polakiewicz J, ´EU law and the ECHR: Will EU accession to the European Convention on Human Rights square the circle?' (Oxford Brookes University, 2013) <http://www.coe.int/t/dghl/standardsetting/hrpolicy/accession/Accession_documents/Oxford_18_January_2013_versionWeb.pdf> Accessed 13 July 2013.

Pring, Johnny, 'Up Close and Personal: Data Protection and EU-US relations", European Policy Centre (2007) < mercury.ethz.ch/.../PB_May07_up_close.pdf> Accessed 1 March 2013.

Schorlemer S, 'Human Rights: Substantive and Institutional Implications of the War Against Terrorism' [2003] (Vol 14 No 2)278 European Journal of International Law < http://ejil.oxfordjournals.org/content/14/2/265.full.pdf> Accessed 1 September 2013.

Wessel, Ramses A., 'The inside looking out: consistency and delimitation in EU external relations', Common Market Law Review [2000] (37: 1135 – 1171) Kluwer Law International http://www.kluwerlawonline.com/abstract.php?area=Journals&id=276760 Accessed 1 August.

Other Documents

Ariel Aaronson S, Internet Governance or Internet Control? How to safeguard Internet Freedom, Cicero Fundation Great Debate Paper No. 13/01 (Gorge Washington University 2013) <http://www.cicerofoundation.org/lectures/Aaronson_Internet_Governance.pdf> Accessed 1 August 2013.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13 (2013).

Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 00062/10 (2010).

Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, 622/10 (2010) .

Article 29 Data Protection Working Party, The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09 (2009).

Article 29 Data Protection Working Party, Opinion 10/2011 on the proposal for a Directive of the European Parliament and the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 00664/11 (2011).

Article 29 Data Protection Working Party, Opinion 5/2012 on Cloud Computing,01037/12 (2012).

Article 29 Data Protection Working Party, Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities, (2007).
Commission ´Communication to the European Parliament and The Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe', COM (2010) 673 final.
Council of Europe ´Guidelines on Human Rights and the Fight against Terrorism', the Committee of Ministers (2002).
Council of the European Union, ´Draft Council Conclusions on an Information Management Strategy for EU internal security' Document 16637/09, (2009).
Council of the European Union, 'Draft Internal Security Strategy for the European Union: "Towards a European Security Model"', (2010).
Council of The European Union, ´EU Counter-Terrorism Coordinator, 'EU Counter-Terrorism Strategy – Discussion paper'', (2012).
European Commission 'Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries', COM (2010) 492 final.
European Commission 'Communication to the European Parliament and the Council, 'Overview of information management in the area of freedom, security and justice'', COM (2010)385 final.
European 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 (notified under document number' C(2004) 1914 (2004/535/EC).
European Commission 'Proposal for a Council Framework Decision, on the use of Passenger Name Record (PNR) for law enforcement purposes' COM (2007) 654 final.
European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes', COM (2011) 32 final.
European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', 2012/0011 (COD), COM(2012) 11 final.
European Commission, 'Proposal for a Directive of the European Parliament and of the Council, on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', 2012/0010 (COD), COM (2012) 10 final.
European Council, 'The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens' (2010)OJ C115/1.
European Data Protection Supervisor, Opinion of 30 September 2010 on 'the Communication from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice"' (2010).
European Data Protection Supervisor, Opinion of 24 November 2010 on 'the Communication from the Commission to the European Parliament and the Council concerning the EU Counter-Terrorism Policy: main achievements and future challenges' (2010)
European Data Protection Supervisor, Opinion of 14 January 2011 on 'the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union"' (2011) OJ C 181/01.
European Data Protection Supervisor, Opinion of 25 March 2011 on 'the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', (2011) OJ C 181/02.
European Parliament, Recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)) OJ C184E/119.
European Parliament, Resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (PE 344.133) (B5-0156/2004) [2004].
European Union Agency for Fundamental, 'Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record data for law enforcement purposes', (2008).
National Security Strategy, Washington, United States, (2010)
<http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf> Accessed 1 August 2013.
Prieto D, 'Working Paper "War about Terror" Civil liberties and national security after 9/11' Council on Foreign Relations (2009) < www.cfr.org/.../Civil_Liberties_WorkingPaper.pdf> Accessed 1 July 2013.
Martin Scheinin, Special Rapporteur on 'the promotion and protection of human rights and fundamental freedoms while counter terrorism', A/HRC/13/37 General Assembly, United Nations, (2009).
Resolution on Privacy by Design, adopted by the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem (2010)27-29.

Trauner, Florian, Occasional Paper 'The Internal-external security Nexus: more coherence under Lisbon?', EU Institute For Security Studies, Paris: March 2011.
United Nations Security Council Resolution 1373 (S/RES/1373) [2001].

Legal Documents

Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, [2012] OJ L186/4.
Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, [2006] OJ L82/15.
Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Brussels, Doc. No. 17434/11, [2012] OJ L215/5.
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] OJ L204/18.
Charter of Fundamental Rights of the European Union, [2010] OJ C 83/02.
Convention based on Article K 3 of the (Maastricht) Treaty on European Union on the Establishment of a European Police Office (Europol Convention), [1995] OJ C316.
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108, Council of Europe, Strasbourg, 1981.
Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60.
Declaration 20 on Article 16 of the Treaty on the Functioning of the European Union, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, [2010] OJ 83/345.
Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, [2010] OJ 83/345.
Directive 95/46/EC, of the European Parliament and of the Council, on the protection of individuals with regard of the processing of personal data and on the free movement of such data, [1995] OJ No L281/31.
Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, [2004] OJ L261/24.
European Convention of Human Rights, [1950] Strasbourg, Council of Europe.
European Parliament and the Council, Regulation (EC) No 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), [2008] OJ 218/60.
International Convention for the Suppression of the Financing of Terrorism, Resolution 54/109, New York: General Assembly of the United Nations, December 1996.
International Covenant on Civil and Political Rights, New York: adopted 16 December 1966, entered into force 23 March 1976. 999 UNTS 171 (ICCPR).
Lisbon Treaty amending the Treaty on the European Union and the Treaty establishing the European Community, signed at Lisbon, [2007] OJ C306/1.
OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, 1980
Universal Declaration of Human Rights, adopted 10 December 1948. UNGA Res 217 A III) (UDHR).

Case Law

Amann v. Switzerland, App no 27798/95 (ECtHR 16 February 200).
Perry v. UK, App no 63737/00, (ECtHR 17 July 2003).
P.G. & J.H. v. UK, App no 44787/98 (ECtHR 25 September 2001).
Joined Cases C-317/04 and C-318/04, Parliament v. Council, [2006] ECR I-4795.
Joined Cases C-402/05 and C-402/05, OJ 2008 C 285/2, Kadi and Al Barakaat International Foundation v Council and Commission, [2008] ECR I-000.
Case T-228/02, Organisation des Modjahedines du Peuple d'Iran v Council [2006] ECR II-4665.
Case T-256/07, People's Mojahedin Organization of Iran v Council, [2008] ECR II-03019.
Case T-284/08 People's Mojahedin Organization of Iran v Council, [2008] ERC II-03487.
Edward Hasbrouck v. U.S. Customs and Border Protection, United States District Court for the Northern District of California, San Francisco Division, order, No. 10-3793 RS.

Media and Others

Commissioner V. Reding, "Your data, your rights: Safeguarding your privacy in a connected world Privacy Platform "The Review of the EU Data Protection Framework", SPEECH/11/183, (Brussels, 16 March 2011)3, available at <http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm> Accessed 1 July 2013.
Bruce Schneier, 'Profiling Makes Us Less Safe, Will profiling make a difference?', The Editors, *The New York Times*, (4 January 2010,) <http://roomfordebate.blogs.nytimes.com/2010/01/04/will-profiling-make-a-difference/> accessed 1 July 2013.

European Parliament News, 'Civil Liberties Committee rejects EU Passenger Name Record proposal', (24 April 2013, <http://www.europarl.europa.eu/news/en/pressroom/content/20130422IPR07523> Accessed 1July 2013.

European Union External Action web site, Statement by H.E. Jean De Ruyt, Permanent Representative of Belgium to the United Nations, on behalf of the European Union, 'Measures to eliminate international terrorism', (New York, 1 October 2002) <http://www.eu-un.europa.eu/articles/en/article_70_en.htm> accessed 1July 2013.

Martin Scheinin, 'Privacy and Security can be Reconciled, *The Guardian* (20 January 2010), <http://www.guardian.co.uk/commentisfree/libertycentral/2010/jan/20/privacy-airport-security> accessed 1July 2013.

Rachman, Gideon, 'Obama should end his reticence on rights', *Financial Times*, (November 26, 2012) <http://www.ft.com/cms/s/0/1f80840e-37bc-11e2-a97e-00144feabdc0.html#axzz2OqJz1qdb> accessed 1 May 2013.

Savage, Charlie and Wyatt, Edward, 'U.S. Confirms that it Gathers Online Data Overseas', *The New York Times*, (6 June 2013) <http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all&_r=0>> Accessed 1 July 2013.

Speech by the European Counter-Terrorism Coordinator, Gilles de KERCHOVE, to the United Nations General Assembly on the occasion of the Review of the UN Global Counter-Terrorism Strategy (New York, 4-5 September 2008) available at <http://www.consilium.europa.eu/uedocs/cmsUpload/speechGANYengldef.pdf> Accessed 1 July 2013.

Speech by Javier SOLANA, High Representative for the EU Common Foreign and Security Policy (CFSP) at the Annual Dinner of the Foreign Policy Association (FPA) on "Europe and America - Partners of Choice" (New York, 7 May 2003)

Speech by Gilles de Kerchove, EU Counter terrorist coordinator - Prague, "Euro-Mediterranean Seminar: Counter-terrorism and human rights", 16-17 (Prague June 2008) <http://www.consilium.europa.eu/uedocs/cmsUpload/speech-Counter-terrorism_and_human_rights_GdK_june_08_rev.pdf> accessed 1 July 2013.

Internet Sources (accessed December 2013)

Council of Europe, <http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp>

European Commission, <http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm>

European Commission, <http://ec.europa.eu/civiljustice/glossary/glossary_en.htm>

European Data Protection Supervisor, <http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en>

European Parliament/ Legislative Observatory <http://www.europarl.europa.eu/oeil/popups/summary.do?id=1188880&t=e&l=en>

European Union website http://europa.eu/legislation_summaries/glossary/freedom_security_justice_en.htm.

European Union website http://europa.eu/legislation_summaries/justice_freedom_security/

European Union website http://ec.europa.eu/justice/data-protection/article-29/

European Union website, http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm.

Information and Privacy Commissioner, Ontario, Canada http://www.ipc.on.ca/english/privacy/introduction-to-pbd/.

Online Oxford Dictionaries, <http://oxforddictionaries.com/>.

The Biography Channel Website, Barack Obama, (2013) http://www.biography.com/people/barack-obama-12782369.

The Organisation for Economic Co-operation and Development (OECD) <http://www.oecd.org/sti/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldatabackground.htm>.

Official website of the Department of Homeland Security, United States and European Union Launch Formal Negotiations for an Agreement to Protect Personal Information Exchanged in the Context of Fighting Crime and Terrorism (29 March 2011) <http://www.dhs.gov/news/2011/03/29/united-states-and-european-union-launch-formal-negotiations-agreement-protect>

US Foreign Policy About.com web site, <http://usforeignpolicy.about.com/od/defense/a/what-is-counterterrorism.htm>