Department of: Political Science *Chair:* Comparative Public Law

EU-USA cooperation on information sharing in the fight against terrorism: the roles of privacy and security, and the cases of the TFTP and PNR agreements

SUPERVISOR

Prof. Cristina Fasone

CANDIDATE

Daria Martina

Student Reg. No. 628442

CO-SUPERVISOR:

Prof. Nicola Lupo

ACADEMIC YEAR 2016/2017

DECLARATION

I hereby declare that this thesis is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information, which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.

Daria Martina

ACKNOWLEDGMENT

The successful completion of this thesis would not have been possible without the support from my family, who has always firmly believed in my potential and contributed directly and indirectly to my success.

My sincere gratitude goes to China Foreign Affairs University and LUISS University, for offering me the possibility of studying one year in China. Moreover, I would like to thank my supervisors at CFAU, Professor Gao Wanglai, for her guidance and expert advice, and at LUISS, Professor Cristina Fasone, for her professional recommendations.

My other mention goes to my friends, for encouraging me in all the various stages of this thesis.

Table of contents

Abstract

The terrorist attack of 9/11, followed by the escalation of the terrorist menace in the West, proved the inefficiency of intelligence agencies. From that moment on, in the light of the exponential improvement in the field of Information Technology (IT) sharing sensitive information became central to the fight against terrorism.

This dissertation analyzes the cooperation on information sharing between the United States and the European Union as a response to the terrorist threat after the terrorist attack of 9/11. The main objective is to understand the role of the values of security and privacy in the development of the bilateral negotiations on the exchange of data.

For this purpose, this dissertation will firstly examine the value of information sharing in the context of the cooperation within security communities. Then, it will analyze the counterterrorist approaches of the USA and the EU, highlighting the convergence and the differences, with a focus on the concept of security. Lastly, it will consider the role of privacy in the two legal frameworks, aiming at evaluating its importance in the context of information-sharing.

Understanding the concepts of security and privacy and contextualizing them in the fight against terrorism in the EU and the USA is necessary to show how the value that the two international actors attribute to security and privacy influences their cooperation on information sharing. While security is a reason to engage in this kind of cooperation, the differences in the legal frameworks concerning privacy prove to be great obstacles to the finalization of agreements that regulate the exchange of data.

Thus, this dissertation argues that while security constitutes a reason to engage in negotiations for sharing information, differences in levels of privacy protection make these negotiations lethargic.

Key words: information-sharing, counterterrorism, USA, EU, privacy, security

Chapter 1 – INTRODUCTION

1.1 Research question: significance and aim

Nowadays, states cooperate in numerous ways, participating in the international arena by making agreements and sharing institutions[1]. In the light of the emergence of new threats, and in particular since the intensification of terrorist attacks in the West, states have started to share more and more information for security purposes through international and bilateral agreements[2]. However, the observation of various agreement-making processes between the United States and the European Union shows that there are barriers to negotiations that prevent the two actors from reaching consensus on how to share information[3].

Most studies explain that security is the main factor that blocks cross-border information sharing. Yet, the literature doesn't recognize security as a factor that may actually boost the exchange of information, consequently failing in indentifying real barriers to information sharing. The purpose of this study is to analyze the emergence of the need to share information and the cooperation efforts in this sense between the European Union and the United States, focusing on the roles of security and privacy.

More precisely, this dissertation analyzes the reasons behind the emergence of international agreements on information sharing and the importance to continue to cooperate in this direction. This dissertation will study in particular the efforts of the United States and the European Union to further improve their bilateral relations in response to the threat of terrorism through information sharing. However, as it will be noticed later in this dissertation, these two international actors face important difficulties in reaching agreements on information sharing. The analysis of the different counterterrorism approaches of the EU and the USA will be crucial for understanding the difficulties behind the agreement-making process on the share of information between these two international actors. In this process, the analysis of the roles of privacy and security is central. This analysis will elucidate on the importance of the domestic legal environment for explaining the level of efficiency of the process of information sharing at international level.

---

[1] Robert O. Keohane, "International Institutions: Can Interdependence Work?", *Foreign Policy,* No. 110 (Spring, 1998).
[2] See: Benjamin Netanyahu, *Terrorism - How the West Can Win* (1986); Kristin Archick, "U.S.-EU Cooperation Against Terrorism", *Congressional Research Service* (July 9, 2010).
[3] See: Daniel Keohane, "The EU and counter-terrorism", *CER* (May, 2005); Marieke De Goede, "The SWIFT Affair and the Global Politics of European Security", *JCMS*, Vol. L, Issue 2 (March, 2012), pp. 214–230.

The research question that this study will try to answer is: how do privacy and security influence the EU-US cooperation on information sharing against terrorism?

Explaining the reason to compare the European Union and the United States is important. The European Union might not be a state, but it is a union of states that share standards in terms of human rights, and the need to combat terrorism. Additionally, cooperation with third parties on information sharing at EU level is relevant insofar as this cooperation may affect the protection of rights. Moreover, though the European Union Member States and the United States have different legal cultures, they share common principles - among which the protection of privacy, or the maintenance of peace and security - as well as counterterrorist objectives. Common interests and shared values, as this thesis will explain later, contribute to the positive development of their bilateral cooperation on terrorism. Information sharing is just one form of cooperation between the EU and the USA which, especially after 9/11, is acquiring particular relevance.

Answering the above question is meaningful for the enrichment of the IR literature on information sharing and the debate on the contrasting values of privacy and security, and will contribute to help international actors to understand the steps they should take to improve cooperation in the field of information sharing.

1.2 Literature review

Currently, there is a gap in the literature concerning the analysis of the so-called 'information revolution' through IR theories[4]. Assessments on information-related issues have been mainly political. Most of the literature that has manifested the interest in studying the role of information focused on states' concern over a possible erosion of national sovereignty and issues of domestic instability[5]. This topics gained attention because globalization and, with it, economic integration and technological development contributed to redefining the concept of national sovereignty[6]. This first part of the literature noticed that, even though globalization inhibits states from fully controlling information flows due to the absence of a global regulator of the Internet, states continue to retain massive amounts of information for security reasons. Academic studies provide different concepts of security. Realists look mainly at national security, and those studies who expand the notion of national security tend to include mainly its economic dimension,

[4] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", *International Political Science Review,* Vol. XXVII, No. 3 (July, 2006), p. 222.
[5] Lisa J. Damon, "Freedom of Information versus National Sovereignty: The Need for a New Global Forum for the Resolution of Transborder Data Flow Problems", *Fordham International Law Journal*, Vol. X, Issue 2 (1986), pp. 260-287.
[6] Joseph A. Camilleri and Jim Falk, *The End of Sovereignty? The Politics of a Shrinking and Fragmenting World* (Aldershot, UK: Edward Elgar, 1992).

especially for "IT-related security threats"[7]. For instance, the increased number of cyber-threats, that has become a significant problem after the development of the Internet, could eventually disrupt the economy of a state and, consequently, its political order. An example of the threat that the progress of IT intrinsically entails is the recent interference of the Russian government in the 2016 presidential elections in the USA. As Sally Yates, former Attorney General, and James Clapper, former director of the national intelligence, testified before the Senate Judiciary Committee and the House Intelligence Committee, Russia tried to help Donald Trump win the elections[8]. Even liberals, who have always included other dimensions of security – be them economic, environmental, human – have identified in economic aspects the costs of inter-state connection.[9] Thus, most researches explain that states retain and want to control flows of information for security reasons, focusing on concepts of national security or on the economic dimension of security.

Another part of the literature does not consider security as a barrier to information sharing. The inconsistency behind the logic of considering security as an obstacle can be explained after an attentive analysis of Nye's concept of national security. Nye defines national security as the absence of threat to major values, as democracy and human rights[10]. In his research, Nye also points out that shared values explain cooperation: when states share "mutual and similar objectives, (…) there can be joint gains from coordination"[11]. But what if security is considered as a shared value? If the maintenance of security represents a shared value, it would also be a reason to engage in international cooperation. Indeed, a second part of the literature does consider security as a shared value and believes in the existence of "security communities"[12], in which cooperation ensures peace. The logic behind the idea of a world dominated by anarchy and the predominance of national security interests over international interests and shared values is inconsistent with reality. Reality shows that security is one of the most important values that are shared within the international community. Remarkably, the maintenance of peace and security at international level is one of the main interests and objectives of the United Nations, as it is the first principle that appears in the Charter of the UN (Art.1). Moreover, it is also one of the primary objectives of many other international organizations, such as the European Union (Preamble, Art. 3 TEU), and the North Atlantic Treaty Organization (Art. 1), as well as a fundamental value and right that appears in the Charter of Fundamental Rights of the EU (Preamble; Art. 6) and the European Convention on Human Rights (Preamble; Art. 5). Thus, being the interest of maintaining security a shared value, it explains the willingness of states to cooperate.

---

[7] J. Eriksson and G. Giacomello, p. 229.

[8] "Yates, Clapper To Testify In Senate Hearing On Russian Election Meddling" , *NPR,* April 25, 2017. Available at: http://www.npr.org/sections/thetwo-way/2017/04/25/525542524/yates-clapper-to-testify-in-open-house-hearing-on-russian-election-meddling.

[9] J. Eriksson and G. Giacomello, pp. 221-244.

[10] Joseph S. Jr. Nye, *Soft Power, The Means to Success in World Politics* (New York: Public Affairs, 2004).

[11] *Ibid,* p.17.

[12] Emanuel Adler, and Michael Barnett, *Security Communities* (Cambridge University Press 1998), p. 3.

This second logic suggests that security might be a reason to engage in negotiations on information sharing. In fact, one way in which states cooperate on security is through the "need to share" approach[13], which has increasingly become a critical part of states' policies after the emergence of asymmetric threats. Several international and bilateral agreements on information sharing were actually agreed upon for security reasons[14]. Hence, the observation of reality doesn't support the literature that considers security as the main factor for retaining information, or, put in other words, an obstacle for information sharing. This part of the literature fails to take into consideration the fact that security can be a reason for international actors to share information, rather than retaining it. However, evidence shows also that processes of international cooperation on information sharing are slow, and it is difficult to reach consensus on a final agreement during negotiations. If, on the one hand, the fact that two actors share values and want to promote similar interests can explain the willingness to cooperate, on the other hand, it's not implied that the process that leads to cooperation will be unimpeded and unchallenging. In order to detect the factors that impede international actors from reaching agreements on information sharing, a more in-depth study of negotiation processes is necessary, since the existing literature not only lacks exhaustive studies on information sharing in general, but also falls short of theoretical results and researches on negotiation processes for the exchange of information. Thus, in cases in which the maintenance of security is an explanation for cooperation on information sharing, what can explain the lethargy of negotiations? This dissertation argues that privacy is a barrier to information sharing. The literature recognizes that the new information era provokes privacy concerns. However, scholars are divided on defining the relation between privacy and security. Part of the literature considers privacy and security as opposing and conflicting values. On the contrary, other academics insist on the fact that those views that oppose privacy and security are misleading. In fact, this second group of scholars talks about a "false trade-off"[15] concerning these two values.

1.3 Methodology and Structure

The theoretical framework of this dissertation is based on two assumptions. The first assumption derives from the two-level game theory, according to which negotiation processes at the international level

[13] Peter P. Swire, "Privacy and Information Sharing in the War on Terrorism", *Villanova Law Review,* Vol. LI (2006), p. 101.
[14] See: Canada- EU PNR Agreement and the EU-USA PNR Agreement (share, storage and analysis of passengers' data to fight terrorism); EU-Canada Security of Information; the strategic Agreements on Co-operation between Europol and the Russian Federation, the Republic of Turkey, and Ukraine to exchange information in order to improve the work of law enforcement authorities in the area of crimes.
[15] Daniel J Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press, 2011).

are influenced by domestic processes of bargaining and vice-versa.[16] Putnam claims that negotiations within a state are participated by different groups that want to promote their interests.[17] Put in other words, the first assumption is that the weight of different domestic interests matters when it comes to the study of international agreement-making processes.

The second assumption is that the international aim and national interest to maintain security facilitates the initiation of negotiations on information sharing. Thus, an increase in the level of perception of security threats speeds up the process of negotiation. Since the purpose of this paper is to investigate on the barriers that impede cross-border information sharing between the EU and the USA, the perception of threats will be taken into account as a control variable throughout the analysis of the Passenger Name Record (PNR) case that will be presented in the last section of this thesis.

The hypothesis is based especially on the first assumption of this thesis, namely that the domestic level is essential for studying negotiation processes of agreements on information sharing. Hence, it is reasonable to believe that there is something at regional level in the European Union and at domestic level in the United States that blocks the bilateral process of negotiations on information sharing at international level. The hypothesis is that the protection of privacy is a barrier to international cooperation on information sharing, thus, two cases characterized by different privacy protection levels should be studied. In order to test the hypothesis, this dissertation will consider the European Union and the United States, which are respectively characterized by a higher and lower level of privacy.

The level of privacy protection is determined by the level of legal protection of privacy, as well as by the performance of privacy enforcement authorities. Different indicators will be taken into account: protection at constitutional level, scope of protection, government surveillance, presence of a data protection authority, but also the role of courts in protecting the rights, the violations of the right to privacy, as well as the abuse of power of law enforcement and national security authorities.

It is also necessary to justify the comparison between the United States and the European Union. Although the EU is not a state, it is for sure a sui generis organization, which has been defined by Robert Schütze as a "middle ground between international and national law"[18]. According to him, the EU possesses a federal essence, due to its peculiar features, as "dual government, dual sovereignty"[19], and at the same time its detachment from dualism and shift to cooperative federalism. Moreover, "if the EU is recognized no longer as an intergovernmental international organization but as a supranational system with its own

[16] Robert D. Putnam, "Diplomacy and Domestic Politics: The Logics of Two-Level Games", *International Organization,* Vol. XLII, No. 3 (1988), pp. 427-460.
[17] *Ibid,* p.434.
[18] Robert Schütze, "From Dual to Cooperative Federalism: The Changing Structure of European Law", *European Journal of International Law,* Vol. XXI, Issue 4 (Oxford University Press, 2010), p.3.
[19] *Ibid*, p. 29.

institutional characteristics and autonomy, then comparison with a political system such as that in the United States (US) becomes essential"[20].

The previous section of this chapter has provided the reader with a theoretical background on the literature on information sharing, pointing at the existing gap in academic studies on the analysis of cross-border information sharing, and on the explanation of the factors that may boost or block this process. This premise is helpful to understand that the concept of security is crucial for studying the role of information sharing in security communities[21] and in the EU-USA bilateral cooperation on counterterrorism.

The second chapter begins by exploring the role of security at the international level, and the development of security communities. Then, it analyzes the development of cooperation in security communities especially following the emergence of the terrorist threat. Lastly, it will consider the importance of the need to share information, as well as the emergence of obstacles in the cooperation on information sharing.

The third chapter will more pragmatically analyze the stance of the United States and the European Union on the phenomenon of terrorism, their counterterrorism approaches and the development of bilateral relations. The analysis of the two different responses of the USA and the EU will make the contrast between security and privacy emerge. This chapter is mainly dedicated to the understanding of the role of security for these two actors taking into account their counterterrorism policies and cooperation. The Terrorist Finance Tracking Program (TFTP) case will be used to provide a concrete example of the different value that the EU and the USA attribute to security.

The fourth and last chapter will introduce the reader to an in-depth study of the legal frameworks on privacy and the regulations of personal data in the United Sates and the European Union, highlighting the substantial differences between the two systems. Next, it will try to emphasize the great influence of the value of privacy in the European Union and explain the reason why it constitutes a barrier for the exchange of information between the EU and the USA. Lastly, the PNR case will be used as a practical example to illustrate the lethargy that characterizes the process of information sharing between the EU and the USA, considering the roles played by both privacy and security in the negotiation process.

[20] Sergio Fabbrini, *Democracy and Federalism in the European Union and the United States* (Routledge, 2005).

[21] Some scholars of international relations argue that communities do exist at international level. The actors that are part of these communities share values, interests, they cooperate and trust each others. Moreover, security politics is largely based on the existence of such communities. In particular, the concept of "security communities" gained relevance thanks to Karl Deutsch and the traditional IR theories on security started to be seriously challenged. He believed that states are able to become so integrated to develop a sense of community in which there is no resort to war, and stable peace is possible. See: Karl W. Deutsch et al., Political *Community in the North Atlantic Area* (Princeton: Princeton University Press, 1957); Emanuel Adler, and Michael Barnett, *Security Communities* (Cambridge University Press, 1998).

Lastly, the fourth chapter will give conclusions on the role of privacy and security in EU-USA bilateral cooperation on information sharing and try to put forward some recommendations and suggestions in the light of the findings.

Chapter 2 – INFORMATION SHARING IN SECURITY COMMUNITIES

2.1 Cooperation in Security Communities

The international political discourse concerning problems of security has been dominated by the realist tradition and its variations. According to realism and neorealism, international politics is characterized by the struggle for power and the prevalence of an anarchic international system in which the principal actor is the nation-state. According to Waltz, the main value that influences states' policies is national security[22]. The traditional concept of security is founded on the security dilemma and the theory of deterrence. States continuously accumulate resources to increase their economic and military powers to make their defense apparatus grow, but the result of this effort generates insecurity in other states. Moreover, deterrence is a strategy that is used by a state to make an adversary think that an attack would cause inacceptable damages rather than benefits. Thus, the traditional realist idea of security focuses on the role of the state and it is strictly related to military security. After the Cold War, the survival of the traditional concept of security was undermined by various changes, among which the menace of Islamic terrorism.

Firstly, the terrorist attacks of 2001 and the subsequent emergence of a transnational problem that involves actors at all levels (NGOs, International Organizations, States, etc) weakened the traditional vision of security linked to national territory. Secondly, the enemies that began to perpetuate the attacks were non-state actors, which replaced the traditional subjects that had been involved in wars until that moment, namely state actors. Thus, the so-called "War on Terrorism" cannot be associated with the traditional idea of war: the boundaries of states do not matter anymore and the traditional means of deterrence are not effective. Many authors refer to a "new terrorism"[23] or "post-modern terrorism"[24], also because of the non-traditional means used to perpetuate an attack (biological, nuclear, etc).

As a consequence of the changing international environment and the emergence of new threats, the entire discourse about anarchy and the prevalence of national interests which dictate national foreign policies became vane. Security proved to be "a main motive for integration"[25]. Right after the two World Wars, history assisted to an era of institution building – see for example the North Atlantic Treaty Organization, the United Nations and the biggest security organization, namely the Organization for Cooperation and

[22] Kenneth Waltz, *Theory of International Politics* (Addison-Wesley, 1987), p. 238.
[23] Mathew J. Morgan, "The Origins of the New Terrorism", *Parameters,* Vol. XXXIV, No.1, (2004), pp. 30-31.
[24] Boaz Ganor, *The Counter-Terrorism Puzzle: A Guide for Decision Makers* (2005), preface.
[25] Emanuel Adler, and Michael Barnett, *Security Communities* (Cambridge University Press 1998), p. 91.

Security in Europe – and to the emergence of "transnational community (…) policymakers"[26] and the so-called "security communities"[27] that shared a common objective: the maintenance of peace and security. In the context of the rising terrorist threat and the new characterizations of terrorism, the already existing international organizational framework for cooperation on security rapidly turned its attention, resources and efforts to repress Islamist ideologies and fundamentalism. New programs specifically focused on terrorism were put in place, and new frameworks for cooperation were created. Monica Den Boer noticed how states are not capable of managing the menace of terrorism by themselves and that, instead, international coordination of anti-terrorist activities works better.[28]

One way in which the security communities began to cooperate was through the share of information and intelligence, but not without difficulties. Indeed, international cooperation on information sharing is influenced by the secrecy that intelligence forces attribute to the information they collect. If the "walls between intelligence and law enforcement agencies" [29] continue to exist, then the effort of International cooperation on sharing information for security purposes is senseless and the exchange can't be efficient. Actually, the problem for this kind of cooperation is not the absence of legislation at international level on this subject: there are conventions and agreements at international level that regulate this cooperation and encourage the share of more sensitive information.

Importantly, NATO has promoted information sharing in response to the terrorist threat, setting up a Terrorist Threat Intelligence Unit (TTIU) which was later replaced by the Intelligent Liaison Unit (ILU), with the aim of exchanging sensitive information with partner countries[30]. More recently, on May 25th 2017, NATO Secretary General Jens Stoltenberg announced that NATO will join the Global Coalition to Defeat ISIS, the result of an initiative of the American government. By doing so, NATO is engaging more and more in the fight against terrorism, and commits to the Coalition by sharing resources, information, logistics and training. Moreover, NATO decided to establish an intelligence cell[31] to ensure a more direct engagement in the fight against terrorism. In 2016, the Security Council of the UN adopted Resolution 2309[32] in which it supported the International Civil Aviation Organization (ICAO) calling the UN members to share more information related to terrorism. As demonstrated by NATO, the European Union, OSCE, the UN, security

[26] E. Adler, and M. Barnett, p. 4.
[27] *Ibid.*
[28] Monica Den Boer, "9/11 and the Europeanisation of Anti-Terrorism Policy: a Critical Assessment", Groupement D'études et de recherches, *Policy Papers*, No.6, (2003), p.19. Available at: http://ftp.infoeuropa.eurocid.pt/files/database/000005001-000010000/000007639.pdf.
[29] Richard A. Best Jr., "Sharing Law Enforcement and Intelligence Information: The Congressional Role", *Congressional Research Service*, February 13, 2007. Available at: https://fas.org/sgp/crs/intel/RL33873.pdf
[30] http://www.natolibguides.info/intelligence.
[31] "May 25, 2017: Secretary General Stoltenberg's Doorstep at the NNHQ", U.S. Mission to the North Atlantic Organization, May 25, 2017. Available at: https://nato.usmission.gov/may-25-2017-secretary-general-stoltenbergs-doorstep-nnhq/.
[32] S/RES/2309, September 22, 2016. Available at: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2309.pdf.

communities do manifest the willingness to share information and cooperate in this sense. However, in order to understand the difficulties that may obstacle this type of cooperation, it is important to first understand the reason why information is so valuable to security communities and what kind of information they are interested to share. The next section will introduce some basic knowledge about the Information Technology environment and data that are considered as being "sensitive" and security-related.

2.2 The value of Information sharing in Security Communities

Before talking about the need for information sharing, it is necessary to provide an introduction to the expression "Information Technology" (IT). IT "is the use of any computers, storage, networking and other physical devices (e.g. telephones, recording tools), infrastructure and processes to create, process, store, secure and exchange all forms of electronic data"[33]. The traditional application of IT has been mainly prominent in the socio-economic context, but after the terrorist attacks of 9/11 that proved the disinformation of the American intelligence agencies, IT application has been extended to the area of security. The American government initiated a series of policies to enhance the communication between intelligence agencies and police forces through the share of information. All around the world, projects for the creation of Information Sharing Environments (ISE) were established in order to facilitate the exchange of information between national organizations and processes of cross-border sharing. The European Police Office (Europol), which will be given space in the next chapter, is an example of the institution-building process due to the increasing need to share. Thus, the practice of sharing information became extremely valuable, especially after the 9/11 attack. For example, strengthening information sharing became one of the main objectives of NATO[34].

When it comes to information sharing for the fight against terrorism, first of all it is necessary to define what kinds of data are valuable for security needs. Intelligence agencies are interested in collecting and analyzing both Big Data and metadata, which are two different typologies of data that, in different ways, serve the same scope. The expression "Big Data" refers to the massive quantity of different typologies of data that are produced by the online users or, put in other words, data related to web surfing. These data are the result of all the online activities of a net-surfer: his researches, his logs-in, his conversations, the information he posts on social media, his purchases. Big Data are stored by private and public entities. The

[33] "Information Technology (IT)", *Search Data Center*. Available at: http://searchdatacenter.techtarget.com/definition/IT, accessed April 4, 2017.
[34] "NATO and the fight against terrorism", Transcript of Ambassador Sorin Ducaru, November 6, 2014. Available at: http://www.nato.int/cps/en/natohq/opinions_114693.htm.

analysis of Big Data has an enormous potential: it has an economic and political potential because it can lead to the understanding of people's preferences, but it can also have a crucial applicability in the field of security. Through the analysis of all data that a person leaves on the Internet, her profile can be reconstructed. In the light of the potential of Big Data, democracies have laws that regulate their use and grant the protection of personal information, which is crucial for the survival of people's liberties. Metadata, instead, are a typology of data that refers to all the information of a communication except for the content. Metadata include information about who communicated with whom, where, at what time, and the duration of a communication. Even the collection of metadata can be used to reconstruct the profile of an individual, without the need of knowing the content of her e-mails or phone calls[35]. Thus, the use and analysis of both Big Data and metadata can be essential for security needs.

However, there is disagreement on the typology of data that have to be stored and the methods used by police forces, information agencies and secret services to process them in order to combat crimes. For example, the United States is more oriented towards an indiscriminate collection of data, while in the European Union the usefulness of a massive amount of personal data that are not collected with rationality is highly doubted. In his opinion on the use of PNR to combat serious crimes[36], the European Data Protection Supervisor Giovanni Buttarelli said that "Europe is facing serious terrorist threats and has to take meaningful action. The combat against terrorism and serious crime is a legitimate interest pursued by the legislator and the EDPS, as an EU independent supervisory institution, is not a priori in favour or against any measure"[37]. Nevertheless, there is no evidence that justifies the need to adopt a system of "massive, non-targeted and indiscriminate collection of data of individuals"[38]. The disagreement between the EU and the USA on the methods used for risk-assessment purposes is mainly due to the increasing amount of concerns on the respect of fundamental rights that has emerged with the information age, not to mention the huge amount of resources needed to collect and analyze Big Data. Though the value of data mining in the fight against terrorism is widely recognized, the indiscriminate collection of data is criticized. Many researchers have great difficulties in identifying the potential of a counterterrorist strategy that relies on the analysis of such kind of data. For example, Jeff Jonas and Jim Harper point out that the American intelligence had huge chances to discover the planning of the 9/11 attack in New York, since two of the terrorists involved in the attack "were already considered suspects by federal authorities and known to be in the United States"[39].

[35] "La società sorvegliata", *Garante Privacy*, Atti del Convegno, January 8, 2016, p. 167. Available at: http://194.242.234.211/documents/10160/5312012/La+societ%C3%A0+sorvegliata+-+Atti+del+convegno+del+29+gennaio+2016.

[36] "Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime", Opinion 5/2015 EDPS, September 24, 2015. Available at: https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf.

[37] *Ibid*, p. 3.

[38] *Ibid*, p. 4.

[39] Jeff Jonas, and Jim Harper, "Effective Counterterrorism and Limited Role of Predictive Data Mining", *Policy Analysis,* No. 584 (December 11, 2006), p. 3. Available at: https://object.cato.org/pubs/pas/pa584.pdf.

Thus, the federal authorities could have used their investigative powers and abilities, and focus their resources on known suspects. "In the days and months before 9/11, new laws and technologies like predictive data mining were not necessary to connect the dots. What was needed to reveal the remaining 9/11 conspirators was better communication (and) collaboration"[40]. Moreover, since 2001, the technologies have evolved and improved and the amount of Big Data that circulate has exponentially increased, and "the more personally identifiable information Big Data systems contain, the greater the potential risk"[41] of potential misuse.

2.3 Obstacles to Information Sharing: finding a balance between privacy and security

In order to understand what kinds of difficulties emerge in the context of information sharing within security communities, it is necessary to briefly introduce the general problem of respecting human rights while combating terrorism. As anticipated, as the threat of terrorism became transnational, also the fight against it acquired international features. The international community has engaged in the fight against terrorist – different from the "War on Terror"- and states cooperate sharing their resources and supporting each others in order to reduce the menace of terrorism. Affirming that the international community joined the War on Terror could be controversial. Indeed, the problem of the theory of the War on Terror is that the menace of terrorism has been used to legitimate state actions that erode the strength of fundamental rights. For example, the CIA was accused of violating international treaties and national laws that prohibit the use of torture. Its torture techniques as waterboarding, as well as the illegal imprisonment and treatment of terrorist suspects in the Guantanamo Bay made worries and indignity spread out within the international community. Apparently, in the fight against terror, there is a threshold of acceptability in the context of human rights respect that can't be bypassed. The problem of eroding rights while combating terrorism affects international organizations, too. An example is the list of terrorists associated with Al-Qaida, which is the result of the decision of the Security Council, and does not entail the possibility of judicial review. Not only is the information used to make the list not thoroughly checked by a supervisory authority, it is also the result of classified data of all the countries that, as a consequence, are not shared within the Council. Martin

[40] *Ibid.*

[41] Ann Cavoukian, and Jeff Jonas, "Privacy by Design in the Age of Big Data", June 8, 2012, p. 7. Available at: https://datatilsynet.no/globalassets/global/seminar_foredrag/innebygdpersonvern/privacy-by-design-and-big-data_ibmvedlegg1.pdf.

Scheinin believes that the creation of a Delisting Ombudsperson does not grant a sufficient level of review, especially because members of the Security Council can overrule the opinion of the Ombudsperson[42].

The observance of the law is seen as a fundamental requirement for the preservation of security and democracy. Generally speaking, fundamental rights are inalienable and cannot be violated. Thus, bypassing fundamental rights, as well as democratic values and fundamental liberties granted by the law at international level for security purposes is unacceptable, even if the case is to combat terrorism. The European Court of Justice (ECJ) ruling on the famous Kadi case[43] illustrates the relationship between the European Community (as it then was) and international law, and it is one of the most significant judgments concerning the protection of fundamental rights[44]. Yassin Abdullah Kadi was a Saudi Arabian who was "suspected of supporting terrorism" according to the EU Regulation 467/2001. Under the 2001 Regulation, all his financial assets that he had in the EU had to be frozen. In 2002, Regulation 467/2001 was replaced by the Council Regulation 881/2002, which was the result of the implementation of some resolutions of the United Nations Security Council (UNSC) that required to freeze the funds and assets of individuals associated with Al-Qaida, the Taliban and Osama Bin Laden[45]. Kadi's name appeared in the list of suspects of the Security Council, and therefore in the annex to the new EU Regulation. However, the UNSC also adopted a Resolution concerning humanitarian exceptions to the previous resolutions on the freezing of terrorists' economic funds (some reasonable expenses were allowed for food, medical care and legal fees)[46]. Following this SC Resolution, the EU amended the Council Regulation of 2002[47] through the Council Regulation (EC) 561/2003 that provided for some permitted expenses. The EU Council and the Commission argued that the EU and its Member States were bound by international law (UN Charter[48]). By adopting an internationalist approach[49] and a monistic consideration of EU law with respect to international law[50], the Court of First Instance (CFI, now General Court) declared the primacy of the UN Charter over the legislation of the Community, referring to Art. 307(01) EC, Art. 297 EC, and to the theory of substitution[51].

---

[42] David Cole, Federico Fabbrini and Arianna Vedaschi, Secrecy, National Security and the Vindication of Constitutional Law (Edward Elgar, 2013), p. x.

[43] *Yassin Abdullah Kadi v. Council of the EU and Commission of the EC*, joined with *Al Barakaat International Foundation v. Council of the EU and Commission of the EC* on appeal to the ECJ. Joined Cases C-402/05 P & C-415/05 P (ECJ September 3, 2008).

[44] P. Takis Tridimas, "EU Law, International Law and Economic Sanctions Against Terrorism: The Judiciary in Distress?", 32 *Fordham Int'l L.J.,* 660 (2009).

[45] Resolutions of the UNSC: 1267(1999); 1333(2000); 1390(2002).

[46] UNSC Resolution 1452(2002).

[47] Regulation (EC) 881/2002.

[48] In particular by Articles 24 and 25 of the United Nations Charter, which provide that the members of the UN agree on conferring on the SC primary responsibility for the maintenance of international peace and security, they agree that the SC acts on their behalf (Art. 24), and they agree to carry out the decisions of the SC (Art. 25).

[49] P. Takis Tridimas, p. 681.

[50] Grainne de Burca, and Joseph Halevi Horowitz Weiler, *The Worlds of European Constitutionalism* (Cambridge University Press, 2011) p. 118.

[51] According to Art. 307 EC, international agreements concluded by the members of the Community before the EC Treaties had to be preserved. According to the theory of substitution developed in *International Fruit Co. NV v. Produktschap Voor Groenten en*

Although the CFI ruled that Kadi's rights had not been violated, the ECJ adopted a constitutionalist and dualistic approach[52], and reversed the judgment of the CFI finding the EU regulations "in breach of the right to a hearing, the right to judicial protection and the right to property"[53]. This judgment was striking insofar as it "represents a significant departure from the conventional presentation and widespread understanding of the EU as an actor maintaining a distinctive commitment to international law and institutions"[54]. Indeed, the case of Kadi is one of the most important precedents to the numerous challenges that have been presented before the courts of the European Union addressing the activities of the UN that harmed individuals' rights[55]. This case demonstrates that, no matter how much the EU is committed to the respect of international law, in particular concerning security issues, fundamental rights cannot be violated.

This premise is necessary to understand the concerns that arise considering the increasing number of initiatives against terrorism that include sharing information, collecting and analyzing data and promoting mass surveillance programs for security purposes.

Baldwin tries to consider security through the prime value approach, the core value approach and the marginal value approach. Applying the prime value approach to security, he concludes that "even if 'absolute' security were a possibility, it is not obvious that people would seek it"[56]. For instance, in the EU it is clear that security does not entail to be restricted, as the Charter of Fundamental Rights refers to security and liberty in the same article (Art.6). The application of the other two approaches is much more complicated. Defining security as a core value moderates the idea of an "absolute" security, for it would be considered as part of a set of core values characterized by relevant importance. However, it would be necessary to justify the exclusion of other values from the set of core values. According to the marginal value approach, security is subject to the law of diminishing returns: being security a policy objective, the resources allocated to security will vary according to the historical moment and the need of security compared to the need of other policy objectives[57]. The effort of weighting the value of security with respect to other values is vane in the eyes of other scholars, especially for neorealists, who see security as the main end.

Fruit (1972), "where under the EC Treaties the Community assumes powers previously exercised by the Member States in an area governed by an international agreement, the provisions of that agreement become binding on the Community" (P. Takis Tridimas, p.680). Therefore, since the MS of the Community were bound by the UN Charter, the powers for the performance of the MS obligations under the Charter had been transferred to the Community.

[52] Grainne de Burca, et al., p.119.

[53] P. Takis Tridimas, p. 661.

[54] Gainne de Burca, "The European Court of Justice and the International Legal Order After Kadi", *Harvard International Law Journal*, Vol. LI, No. 1 (2010), p. 2.

[55] *Ibid*, p. 4.

[56] David A. Baldwin, "The concept of security", *Review of International Studies*, No.23 (1997), p. 19. Available at: http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf.

[57] *Ibid,* pp. 19-20.

As Rory J. Conces notices, classical realists and neo-realists have struggled to strengthen the role of realism looking for moral justifications. He develops on the idea of David Chandler that the Western states' foreign policies have shifted their attention on human rights issues.[58] For Conces, realism can be moralized, and he pushes for a rethinking of realism to include moral principles in the concept of national interest. However, the moral grounds that have been used to support national interests should be deeply justified and should be reasonable. This means that the preference of the value of national security may have effects on other fundamental values. Thus, the choice of security over other values must be explained.

In the context of the fight against terrorism, the debate about the contrast between security and human rights intensified, focusing in particular on the value of privacy since it plays a decisive role in the era of information.

In 1985, the sociologist Gary Marks supported the idea that technology is eroding the barrier to the nightmare of a totally controlled society. The more IT technology develops, the more people more or less consciously make their personal data available. We talk about personal information that people share on social networks, data that are collected for commercial purposes, chronology of internet, images and footages captured by video surveillance, etc. New sophisticated technologies are considered as positive for the progress and development of humanity. However, the use of those technologies leaves many little traces about the life of a person that can be put together in order to reconstruct segments or even the entire life of that person, depending on the allowed storage time of information. Essentially, this is the profiling activity of intelligence agencies that was anticipated in the last paragraph. Of course, the huge potential that data have leads to the need of protecting servers that store data. In this, cyber security plays a fundamental role. Not anyone can have access to these data. States, as well as agencies and companies have justified the storage and use of data for security purposes. The massive quantity of personal data that are retained by both the private and the public sectors, are used by states not only to track criminal activities, but also to prevent crimes and even to assess risks about potential crimes. What is currently happening is that these data are examined to reduce risks, whether a risk is serious at the point that it could endanger an entire society, or not really harming. For example, China is trying to create a system of data analysis with the purpose of rating the reliability of people for granting loans.[59] The Vice President of the Italian Data Protection Authority Augusta Iannini firmly believes that the effect of the current strict control by societies turns people into numbers, so people are mathematized with the aim to create safer societies. This opinion is supported by the intrinsic features of Information Technology. According to Leavitt and Whisler, the application of IT includes "statistical and mathematical methods to decision-making problems, (and) (...) the simulation of

[58] Rory J. Conces, "Rethinking Realism (or Whatever) and the War on Terrorism in a Place like the Balkans", *Theoria. A Journal of Social and Political Theory,* No. 120 (2009), p.2. Available at: http://www.kakanien-revisited.at/beitr/theorie/RConces3.pdf.
[59] "La società sorvegliata", *Garante Privacy*, Atti del Convegno, January 8, 2016, p. 14. Available at: http://194.242.234.211/documents/10160/5312012/La+societ%C3%A0+sorvegliata+-+Atti+del+convegno+del+29+gennaio+2016.

higher-order thinking through computer programs"[60]. These possibilities of application of IT have been used to profile people in the context of security. However, this process is negatively affecting civil liberties, leading to an authoritarian control of information and people. Thus, the idea of a controlled society has grown in parallel with the scientific improvements in informatics and technology. Such kind of control would certainly result in a decline in privacy and democracy. A "Big Brother" society as described in Orwell book 1984 is an extreme that many seem afraid of, especially in democratic states.

Considering the increasing importance of sharing information and the concerns that surveillance provoke, the discussion on privacy and security gains significance and centrality. This is due to the fact that " if "security" doesn't work as a reason not to share, then privacy is offered, as the reason not to share"[61].

Privacy is a right that is recognized in all modern societies. Remarkably, privacy is recognized as a fundamental human right in two international treaties: Art. 12 of the United Nations Declaration on Human Rights (UDHR) and Art. 17 of the International Covenant on Civil and Political Rights (ICCPR). Additionally, the right to privacy is included in several other international conventions and declarations and it is also protected at national level, which may grant a higher level of privacy protection. The right to privacy protects the properties and communications of people from external interference. It helps people defend themselves from abuses of power and grants them liberty.[62] For any organization, information is so valuable that systems of protection are needed. Organizations must assure the confidentiality of users' information, and protect it from unauthorized access, thus, avoiding personal privacy issues.[63] In an era of technological advances, the protection of personal data seems central. The right to protection of personal data can be derived from the general right to privacy. Especially after the emergence of asymmetric forms of terrorism and transnationalization of organized crime, the volume of data subject to surveillance policies has expanded, also thanks to technological improvements. Consequently, many other legislative instruments have been introduced to regulate the collection, storage, access and processing of personal data.[64]

The questions that arise in the debate on privacy and security are the following: is the choice between security and privacy really a choice? On what grounds may a state possibly choose between privacy and security? What value prevails over the other?

---

[60] Harold J. Leavitt and Thomas L. Whisler, "Management in the 1980's", *Harvard Business Review* (November, 1958). Available at: https://hbr.org/1958/11/management-in-the-1980s.

[61] Maureen Baginski, "Intelligence Policy and the Science of Intelligence", *Protecting Persons While Protecting the People,* eds. Cecilia S. Gal, Paul B. Kantor, and Michael E. Lesk (Springer, 2009), p.13.

[62] "What is Privacy?", *Privacy International.* Available at: https://www.privacyinternational.org/node/54.

[63] Kwo-Shing Hong, Yen-Ping Chi, Louis R. Chao, and Jih-Hsing Tang, "An integrated system of information security management", *Information Management & Computer Security,* Vol XI, Issue 5, (2003) p. 243. Available at: http://kczx.shupl.edu.cn/download/85fbe28e-f3a4-4765-a41a-95f5b71d2c31.pdf.

[64] See for example: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; or Convention 108 of the Council of Europe.

Those who support the idea of the primacy of security as a fundamental value use very powerful arguments to make people believe that giving up part of their privacy is necessary to achieve a safer environment. Opposing views to the arguments about the primacy of security try to demonstrate that the idea of choosing between the values of privacy and security is misleading. This category supports the theory of a "false tradeoff", arguing that the idea of a tradeoff between the two values is based on false assumptions. Daniel J. Solove argues that "it is possible to have potent security measures and to protect privacy too, since protecting privacy doesn't entail scrapping security measures but demands only that they be subjected to oversight and regulation."[65] Hence, privacy and security are two values that are not necessarily in contrast with each other, in the sense that they can coexist in a society. As this dissertation will further clarify later, the case of the European Union perfectly exemplifies the possibility of coexistence of privacy and security, which are both fundamental values and enjoy a very high level of protection.

On the other hand, the idea of privacy and security as mutually exclusive values may be due to different reasons. Firstly, security necessities are much more understood by people than privacy needs. Security has been defined as an inalienable public good[66], while privacy is underestimated and treated as a value belonging to the individual. Solove's argument is that privacy is a "societal value"[67], and sometimes legal systems don't provide for a sufficient level of protection of privacy. This reasoning is particularly evident in the case of the United States, where the value of national security has always been preferred to the value of privacy.

However, it is very controversial to affirm that privacy and security are perfectly compatible values. Even in the case of the EU, where privacy is very much protected, contrasts between security and privacy issues frequently emerge. However, the analysis of the EU legal framework and the protection that it grants to privacy is necessary to understand the fact that a high level of privacy protection does not undermine its regional security.

In the next chapter, it will be much clearer that privacy issues in the United States are mostly due to lack of transparency and oversight of the government. Indeed, in this debate about privacy and security, disinformation and lack of transparency and control are central. Correct information about the value of privacy and the meaning of renouncing to this value is fundamental in order to let people understand the real effects of a possible loss of privacy or a trade-off between privacy and security. Moreover, transparency about the processing of personal data is crucial to increase the awareness of people on how much of their life

[65] Daniel J Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press, 2011), p. 14.
[66] "La società sorvegliata", *Garante Privacy,* Atti del Convegno, January 8, 2016, p. 25. Available at: http://194.242.234.211/documents/10160/5312012/La+societ%C3%A0+sorvegliata+-+Atti+del+convegno+del+29+gennaio+2016.
[67] D.J Solove, p. 15.

is exposed. Lastly, supervision is necessary to impede and detect eventual abuse of power which may disregard the right to privacy.

Chapter 3 – COUNTERTERRORISM AND EU-US INFORMATION SHARING: THE VALUE OF SECURITY

After the terrorist attacks that the EU Member States and the United States have experienced, the European Union and the USA have become very active in the fight against terrorism. These events represent "critical junctures"[68] that influenced the policies of the two actors and their new engagement in and attention to the subject of anti-terrorism. However, their cooperation in the fight against terrorism has not always been easy, especially because of their extremely different responses to terrorism. While the United States adopted a hard approach[69], the European Union preferred a regulatory or legal approach.

The differences in their counterterrorism approaches are partly due to new technological developments, which have given to terrorists new instruments. The Net is necessary to spread terrorist messages and recruit foreign fighters, and greatly minimized the problem of distance. How much resolute is a military attack in a foreign country where a terrorist group has headquarters considering that terrorist cells are spread all around the world? Individuals that agree with the message of Islamic terrorism can easily act on their own. The easiness of perpetuating a terrorist attack is demonstrated by the recent tragedies of Nice, Stockholm, Berlin, Manchester and London. In less than a year, terrorists were able to attack the European countries by simply driving vehicles into crowds.[70] The ability to organize a terrorist attack is one of the two essential requirements of Ganor's Terrorism Equation[71]. The other element is the existence of a motivation. The elimination of the motives that stand behind an attack, and in general behind radicalization processes, would have a significant impact on the evolution of terrorism. However, Ganor is well aware of the fact that this task is not easy. The difficulty of adopting a soft-counterterrorism approach through deradicalization programs may lead governments towards the preference of a hard approach. This was the case for the United States, whose choice was also determined by the existence of a cultural strategy based on national security. However, such choice is not effective and may lead to a further increase of radicalization, instead[72]. Even the United Nations' position on counter-terrorism is against hard approaches. In the 2016 General Assembly's

[68] Ruth Berins Collier, and David Collier, *Shaping the political arena: critical junctures, the labor movement and regime dynamics in Latin America* (Princeton: Princeton University Press, 1991), p. 29.
[69] Bruce Hoffman, "Is Europe Soft on Terrorism?", *Foreign Policy*, No.115 (1999), p.64.
[70] Luca Romano, "Nizza, Berlino, Londra, Stoccolma. Gli attacchi terroristici con camion e auto", *il Giornale.* Available at: http://www.ilgiornale.it/news/mondo/nizza-berlino-londra-stoccolma-attacchi-terroristici-camion-1383630.html.
[71] Gabriel Hoeft, "'Soft' Approaches to Counter-Terrorism: An Exploration of the Benefits of Deradicalization Programs", *International Institute for Counter-Terrorism* (2015), p.4. Available at: https://www.ict.org.il/UserFiles/ICT-Soft-Approaches-to-CT-Hoeft.pdf.
[72] *Ibid.*

resolution entitled "The United Nations Global Counter-Terrorism Strategy Review"[73], multilateralism and the legal approach prevailed. The UN members were called to strengthen cooperation and share information[74] to limit the finances of terrorism.

The next paragraph will be dedicated to the study of the American and European approaches to counterterrorism.

3.1 EU-USA Counterterrorism Approaches

Even if the fight against terrorism has gained global attention, there is no global governance for anti-terrorism, yet. The reason is that the interest of repressing terrorist cuts through so many countries with different historical, political and social backgrounds and different legal frameworks that the wish to elaborate an international regulation is very unlikely, at least at the moment. Due to these differences, the strategies and reactions of a country towards the threat of terrorism can be very diverse. The literature on counterterrorism recognizes two different approaches, which are not necessarily mutually exclusive: the military approach and the legal approach. The United States and the European Union approaches to counterterrorism were very different in the first years following the New York terrorist attack. While the United States adopted a "national security" and unilateral approach, the European Union relied on multilateralism.[75]

The 9/11 events had a huge impact on the United States, leading to the reaffirmation of the national security strategy, which reinforced the militaristic approach of the Bush Administration. The United States declared war on terrorism and began to invest a massive amount of resources on defense policies. As anticipated, the military and the legal approaches can coexist. Indeed, in the USA the national security structure rapidly changed and new agencies were created. In 2001, President Bush created the Department of Homeland Security (DHS), a supra-agency whose main aim is to prevent and fight terrorism, and to take the necessary measures to relieve the country from an eventual attack[76]. However, the response of the United States was overall stronger than the EU response in terms of the prevalence of the use of force and national security justifications used to pass legislation which was subsequently criticized for disrespecting human

[73] A/RES/70/291 (July 1, 2016).
[74] "General Assembly Adopts Resolution Affirming Importance of Balanced, Integrated Implementation of Global Counter-Terrorism Strategy", *UN Press*, GA/11800, July 1, 2016. Available at: https://www.un.org/press/en/2016/ga11800.doc.htm.
[75] Wyn Rees and Richard J. Aldrich, "Contending cultures of counterterrorism: transatlantic convergence or divergence?", *International Affairs*, Volume LXXXI, Issue 5 (2005), pp. 905-923.
[76] Larry J. Siegel, *Criminology: Theories, Patterns, and Typologies*, 12th ed (Cengage Learning, 2015), p.399.

rights. Indeed, the Congress soon expanded the powers of the intelligence and law enforcement authorities with the USA PATRIOT Act[77], and initiated activities of mass surveillance[78] and secret programs of indiscriminate data collection and analysis. Moreover, the Bush Administration passed the Authorization for Use of Military Force[79] (AUMF) in 2001, with which authorized the use of force against the perpetuators of the 9/11 attack.

The USA also introduced the notion of "unlawful enemy combatant" through the Military Commission Act of 2006[80]:

"(i) a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States or its co-belligerents who is not a lawful enemy combatant (including a person who is part of the Taliban, al Qaeda, or associated forces); or (ii) a person who, before, on, or after the date of the enactment of the Military Commissions Act of 2006, has been determined to be an unlawful enemy combatant by a Combatant Status Review Tribunal or another competent tribunal established under the authority of the President or the Secretary of Defense"[81].

Additionally, through the Executive Order 13440 of 2007[82], the Bush Administration established an interpretation for the Geneva Convention, which was abandoned during the Obama Administration for being incorrect. The Executive Order provided that all the forces and terrorists associated with Al-Qaida and the Taliban were "unlawful enemy combatants". Falling within this category would mean that terrorists, being illegal combatants and not respecting the laws of war, could not be considered as "prisoners of war" and, thus, be protected by the Geneva Convention which regulates "case(s) of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties"[83], and provides that all the persons not taking "active part in the hostilities"[84] (for instance due to detention) should be treated humanely and respectfully. The Executive Order also disregarded the fact that cruel and degrading treatment of detainees are prohibited under title 18 of the United States Code, the Military Commission Act and the Detainee Treatment Act of 2005, but also more in general by the Fifth, Eight and Fourteenth Amendments to the USA Constitution.

---

[77] USA PATRIOT Act is an acronym for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. Pub. L. 110-55, Aug 5, 2007. Text available at: https://www.justice.gov/archive/ll/docs/text-of-paa.pdf.

[78] Robyn R. Mace, "Intelligence, Dataveillance, and Information Privacy", *Protecting Persons While Protecting the People,* eds. Cecilia S. Gal, Paul B. Kantor, and Michael E. Lesk (Springer, 2009), p.36.

[79] Pub. L. 107-40.

[80] Pub. L. 109/366, Oct 17, 2006. Text available at: https://www.loc.gov/rr/frd/Military_Law/pdf/PL-109-366.pdf.

[81] *Ibid*.

[82] EO 13440, July 20,2007. Text available at: https://fas.org/irp/offdocs/eo/eo-13440.htm.

[83] Geneva Convention (III), Part I, Art. 3. Text available at: http://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.32_GC-III-EN.pdf.

[84] *Ibid*.

Concerning the EU, even though it is a union of states, Member States (MS) are bound by EU law and the EU has a fundamental role in issues concerning security. It is true that national security remains a power of each member-state, as provided by Art. 4(2) of the Treaty of the European Union, which states:

"[t]he Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State"[85].

Even if EU MSs are responsible for issues of national security, article 42 provides for a common foreign and security policy[86]. However, the European Union has never experienced a national security culture. The first reason is clearly that the European Union comprises many states that are characterized by diverging pasts. As for past terrorist concerns, some Member States of the EU experienced terrorism, even if it was another typology of terrorism. For instance, Italy and Spain experienced internal political terrorism. However, terrorist threats have been domestically managed. Differently from the United States, the response of the European Union mainly entailed a regulatory approach, which is supported and preferred at international level. Remarkably, the Security Council Resolution 1373[87] required all the members of the United Nations to adopt new national legislation against terrorism. The European regulatory response has also been referred to with other expressions as "legal" or "institutionalised"[88]. These expressions well represent the type of action that the European Union adopted against terrorism. Indeed, the EU has established an institutional system that is characterized by control mechanisms, strategies, conventions, and legal instruments for preventing terrorist attacks[89]. When, in 1993, the European Union was created next to the European Community by the Maastricht Treaty, no attention was devolved to the creation of a "European military". However, a European Police Office was established by the Maastricht Treaty with the aim to help the members of the EU to contrast terrorism and other forms of serious crimes, by "promoting co-operation among law enforcement authorities of the EU Member States"[90]. This agency is founded on a system of accountability, which includes the European Parliament, but also the European Court of Auditors, the Internal Audit Service and the Internal Audit Function for financial accountability, and the European Ombudsman who acts as a

[85] Consolidated version of the TEU, TITLE I, Art. 4(2).
[86] TEU, TITLE V, Chapter 2, Section 2, Art. 42.
[87] UN Doc S/RES/137 (28 September 2001).
[88] Lee Jarvis, Stuart MacDonald, and Thomas M Chen, *Terrorism Online: Politics, Law and Technology* (Routledge, 2015).
[89] Examples of the regulatory approach are: 2008/919/JHA Framework Decision; Convention on the Prevention of Terrorism of 2005, Cybercrime Convention of 2001, Committee of Experts on Terrorism, numerous EU Counterterrorism Strategies, Counter Terrorism Task Force, Europol, Eurojust, European Arrest Warrant, etc.
[90] Davide Casale, "EU Institutional and Legal Counter-terrorism Framework", *Defense Against Terrorism Review*, Vol. I, No.1 (2008), p. 55.

watchdog for the administration transparency and the accountability[91]. In order to strengthen its operations against terrorism, the Europol founded in 2016 the European Counter Terrorism Center, which is currently helping European countries with the investigations on the recent terrorist attacks. Europol also cooperate with Eurojust, another European agency that was established in 2002. Eurojust provides assistance to the competent authorities of EU Member States for investigations and prosecution activities dealing with serious crimes. While the Europol and Eurojust are mainly responsible for enhancing the cooperation among competent authorities in order to better face the threat of terrorism, the creation of another body has been advanced by the Commission to start investigations against financial offences "relating to participation in a criminal organization"[92], namely the European Public Prosecutor's Office (EPPO). These bodies exemplify the preference of the European Union for an institutional approach against terrorism. Moreover, the European Union criticized the urgency of the USA to insist on the use of force, a practice that is internationally disregarded and that had not proven to be successful in the past. Indeed, as anticipated, fundamental rights cannot be ignored for security purposes, even in the emergency status created by terrorism.

3.2 EU-USA Cooperation on counterterrorism

In general, the cooperation on terrorism between the USA and the EU has improved since the 9/11 attacks, so this section will try to elucidate on the reasons that enhanced bilateral cooperation. As previously noticed, the European Union preferred a regulatory or legal approach against the threat of terrorism. For the European Union is essential to respect the rule of law and fundamental rights. The national security urgencies of the United States, instead, led to the disregard of fundamental rights. Indeed, in the immediate aftermath of 9/11, the executive branch started to violate the protections guaranteed by the U.S. Code and the Geneva Convention[93]. Remarkably, in 2002 José Padilla, an American citizen who was helping terrorists, was labeled "enemy combatant" in a presidential order to Secretary Rumsfeld, brought to a military prison and subject to harsh techniques like prolonged solitary confinement, violating the Geneva Convention[94].

[91] See also: https://www.europol.europa.eu/about-europol/accountability.
[92] "Towards a European Public Prosecutor's Office (EPPO)", LIBE Committee (EU, 2016). Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571399/IPOL_STU(2016)571399_EN.pdf.
[93] See: Rumsfeld v. Padilla, 542 U.S. 426 (2004); Hamdi et al v. Rumsfeld et al, 542 US 507 (2004).
[94] See also: "Petition Alleging Violations of Human Rights of José Padilla and Estela Lebron by the USA with a request for investigation and hearing on the merits", available at: https://www.aclu.org/files/assets/iachr_padilla_petition.pdf.

Moreover, the Supreme Court just found that the case had been improperly filed, not ruling on the legality of the imprisonment of Padilla under the AUMF[95].

The preference of the value of security by the USA surely affected the international image of the nation. In the eyes of the European Union, the American government's violations were inacceptable.

It is obvious that since the European Union and the United States have different approaches and adopt different policies to combat terrorism, bilateral cooperation is not simple. After 9/11, in spite of the difficulties, bilateral relationship began to improve because of the state of emergency and the panic that the attack spread within the international community. Indeed, it was right after the 9/11 terrorist attack that the cooperation between the EU and the USA started, with a proposal of an agreement between Europol (the EU law enforcement agency for the cooperation among police forces) and the American government on the exchange of data. Moreover, the move of Condoleezza Rice from the National Security Council (NSC) to the State Department in 2005 marked a change in the strategy of the US, which began to embrace more cooperation and multilateralism[96] (for instance, through the 2006 National Military Strategic Plan for the War on Terrorism that promoted interconnectedness and cooperation) and the military approach began to be criticized even within the USA. Additionally, the change of the Administration after the presidential elections of 2009 determined an upgrade of the international status of the USA and, in turn, a shift in the relationship with the European States. Among other objectives, the agenda of the new President Barak Obama included the closing of Guantanamo, the end of the war in Iraq and nuclear disarmament. Obama revoked Bush's Executive Order 13440 of 2007, which had pushed the CIA to adopt harsh methods and coercive interrogation on "enemy combatants"[97] (Section 3.1), violating the Geneva Convention. Obama's agenda seemed to promote multilateralism in the governance of security, going beyond the traditional security framework of NATO. All these initiatives made the European Union consider the new aims of the USA as perfectly coinciding with the 2003 European Security Strategy objectives[98], as well as with the 2010 Stockholm Programme[99] for the strengthening of EU relations with third parties, especially in relation to security matters.

Even though Obama campaigned against many of Bush's domestic and foreign security operations, and proposed a different agenda, there have been some continuities with the precedent policies[100]. An example is the use of force and the authorization of strikes in Pakistan, Somalia and Yemen against

[95] Rumsfeld v. Padilla, 542 U.S. 426 (2004).
[96] Álvaro de Vasconcelos and Marcin Zaborowski, "The Obama Moment: European and American Perspectives", *EU Institute for Security Studies* (2009), p. 68. Available at: http://www.iss.europa.eu/uploads/media/The_Obama_Moment__web_A4.pdf.
[97] The expression that was used in the Presidential Order referred also to terrorists.
[98] Álvaro de Vasconcelos and Marcin Zaborowski, "The Obama Moment: European and American Perspectives", *EU Institute for Security Studies* (2009), p.14. Available at: http://www.iss.europa.eu/uploads/media/The_Obama_Moment__web_A4.pdf.
[99] "The Stockholm Programme", *Eur-Lex*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Ajl0034.
[100] Richard Jackson, "Culture, identity and hegemony: Continuity and (the lack of) change in US counterterrorism policy from Bush to Obama", *International Politics,* Vol. XLVIII (March 2011), pp. 390-411.

suspected terrorists[101]. But more crucially, he authorized the military intervention in Libya in order to overthrow Gaddafi's regime. Moreover, Obama was found as responsible as Bush for the intelligence agencies' mass surveillance programs that threatened the privacy of American citizens[102]. "It is clear that (the Obama administration) has attempted to balance both realist and liberal thinkers within its ranks"[103], creating a "Hybrid National Security Doctrine"[104].

So overall, one cannot affirm that there have been huge differences between the two American administrations. Consequently, the difficulty that characterizes the collaboration of the US and the EU on counterterrorism initiatives is still significant and the improvement of the relationship is very slow. This can be due to the fact that, as Rees and Aldrich affirm, while a shift in strategic doctrines is possible, a significant change in strategic cultures is rare[105]. Strategic cultures are based on the past experience of a country, which is the key determinant of national threat perceptions and of the subsequent policies that are adopted in response to those perceptions. As noticed above, the realist ideology that has always been dominant in the USA had a significant impact on the policies of Obama's Administration, especially concerning issues related to security and the "War on Terror". However, the liberal ideology that enabled Obama to take some steps towards the promotion of multilateralism and the respect of the International Law, allowed a more successful dialogue with the EU and led to a gradual convergence of counterterrorist strategies.[106]

3.3 The TFTP case

The study of the Terrorist Finance Tracking Program is a pragmatic example of the hard-approach that was initially adopted by the United States after 9/11, and of the changing strategy towards multilateralism that characterized the Obama Administration, which enabled more cooperation with the European Union.

---

[101] Tom Curry, "Obama continues, extends some Bush terrorism policies", *NBC News*, June 6, 2013. Available at: http://nbcpolitics.nbcnews.com/_news/2013/06/06/18804146-obama-continues-extends-some-bush-terrorism-policies?lite.

[102] Michael Sainato, "Former NSA Senior Analyst Blasts Obama and Bush for Enabling Deep State Crisis", *Observer*, September 3, 2017. Available at: http://observer.com/2017/03/nsa-senior-analyst-deep-state-crisis/.

[103] "Critically assess the similarities and differences in foreign policy between the administrations of George W. Bush and Barack Obama", *Clumpjack*, January 16, 2015. Available at: https://clumpjack.wordpress.com/2015/01/16/critically-assess-the-similarities-and-differences-in-foreign-policy-between-the-administrations-of-george-w-bush-and-barak-obama/.

[104] Stanley A. Renshon, *National Security in the Obama Administration: Reassessing the Bush Doctrine* (Routledge, 2010), p. 4.

[105] Wyn Rees and Richard J. Aldrich, "Contending cultures of counterterrorism: transatlantic convergence or divergence?", *International Affairs*, Volume LXXXI, Issue 5 (2005), p. 2. Available at: http://wrap.warwick.ac.uk/931/1/WRAP_Aldrich_0672848-240609-00.contendingct.rees.aldrich.9septx.pdf.

[106] Laura C. Ferreira-Perreira and Bruno Oliveira Martins, *The European Union's Fight Against Terrorism: The CFSP and Beyond* (Routledge, 2014), p. 49.

Following the terrorist attacks to the Twin Towers, the United States became of course particularly concerned with the failure of its intelligence. As a consequence, apart from restructuring the internal system of intelligence agencies, the USA Department of the Treasury (DOT) initiated the Terrorist Finance Tracking Program (TFTP) in 2001. Initially, the TFTP was a secret program that obliged financial institutions operating in the USA to share all the information on financial transactions through "administrative subpoenas" issued by the DOT. Administrative subpoenas are also called National Security Letters (NSLs), and they are used by the Department of the Treasury to obtain business records.[107] What the TFTP did, was to loosen up the conditions to obtain administrative subpoenas, facilitating the access to financial records[108]. Disregarding these subpoenas would have meant to get sanctioned by the authorities. However, the range of obtained information was very wide: not only could the authorities have information on transactions within the US, they could also get information on operations towards the USA as well as outside the USA[109].

Worldwide, most financial transactions data are collected in the network of a Belgian company called Society for Worldwide Interbank Financial Telecommunication (SWIFT). Since this company had offices in Virginia (USA), it was subject to the orders of the administrative subpoenas. SWIFT cooperated with the United States until 2003, when it started to manifest concerns because of the high level of confidentiality required by the US, the lack of reassurances by the American authorities about the selectivity of their requests and also because of the lack of a supervising authority.

In June 2006, however, some American newspapers reported the existence of the TFTP and the monitoring activities of the government[110]. This leak was particularly felt in the European Union, mostly because the European Central Bank, which was one of the main supervisors of SWIFT, was aware of the TFTP[111]. Indeed, the European Parliament passed a Resolution[112] in which it expressed its worries for the TFTP and disapproved the secrecy of any operations that concerned the privacy of the Europeans. Moreover, according to the opinion of the Belgian Data Protection Authority, SWIFT's transfer of data operations

---

[107] John Ip, "Terrorism laws and constitutional accountability", in Routledge Handbook of Law and Terrorism, Genevieve Lennon, and Clive Walker (eds), (Abingdon, OX: Routledge, 2015), p.102.

[108] *Ibid*.

[109] "Swift Statement on compliance policy". Available at: http://www.swift.com/index.ctm?item_id=59897.

[110] See: Eric Lichtblau, and James Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror", *New York Times*, June 23, 2006. Available at: http://www.nytimes.com/2006/06/23/washington/23intel.html; Glenn R. Simpson, "U.S. Treasury Tracks Financial Data In Secret Program", *Wall Street Journal*, June 23, 2006. Available at: https://www.wsj.com/articles/SB115101988281688182; Josh Meyer, and Greg Miller, "Secret U.S. Program Tracks Global Bank Transfers", *Los Angeles Times*, June 23, 2006. Available at: http://articles.latimes.com/2006/jun/23/nation/na-swift23.

[111] See: European Parliament resolution on the interception of bank transfer data from the SWIFT system by the US secret services P6_TA(2006)0317; Opinion 10/2006 (WP128) on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), Novermber 22, 2006, p.14. Available at: http://www.dataprotection.ro/servlet/ViewDocument?id=234.

[112] European Parliament resolution on the interception of bank transfer data from the SWIFT system by the US secret services (P6_TA-PROV(2006)0317).

violated national law[113]. Also according to the opinion of the Data Protection Working Party established by Article 29 of the Directive 95/46/EC, the transfers violated different articles of the Directive, as well as the Belgian law[114]. It wasn't until 2007 that the USA and the EU reached an agreement providing for additional guarantees that the USA had to assure for the respect of the European laws on privacy, as the appointment of a European person with monitoring powers[115]. However, due to the continuing concerns that were raised in the EU, SWIFT decided to stop operating in Virginia, thereby subtracting itself from the obligations of the TFTP and subpoenas. This forced the USA to initiate negotiations with the EU in order to access SWIFT data.

Thus, in 2009 the Commission started to draft an interim agreement[116] (EU-US SWIFT Interim Agreement - Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program)**,** which would have granted access to SWIFT's data to the US, under some conditions that protected Europeans' privacy right. Although this time the Parliament expressely requested to be consulted during the negotiations, it was not involved[117]. Indeed, the Commission pushed for the finalization of the interim agreement before the entry into force of the Lisbon Treaty on December 1st, 2009, trying to deprive the Parliament from its co-decisional power which was granted by the Lisbon Treaty (Art.218(6) TFEU). The Council managed to conclude the agreement on November 30th, 2009, bypassing the co-decisional power of the Parliament[118]. At the end of January, a few days before the entry into force of the interim agreement, the text was sent to the Parliament. On February 4th, 2010, the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (LIBE) affirmed that the agreement did not respect privacy rights, and recommended the rejection of the agreement. Thus, the European Parliament rejected the SWIFT Agreement on February 11th. Soon, after the Commission manifested the interest in the conclusion of a new permanent agreement in a Recommendation to the Council[119], a new round of negotiation started between the US and the EU. Thus, the EU and the USA opened negotiations on a new

[113] Available at: http://privacycommission.be/communiqu%E)s/AV37-2006.pdf.

[114] Press Release on the SWIFT Case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), November 23, 2006, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2006/pr_swift_affair_23_11_06_en.pdf.

[115] See: 2007/C 166/09 "Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes — SWIFT". Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1416847896590&uri=CELEX:22007X0720(02).

[116] The word *Interim* refers to the temporary nature of the agreement.

[117] Maria Romaniello, "The international role of the European Parliament: the SWIFT Affair and the 're-assessed' European institution balance of power", *Perspectives on Federalism,* Vol. V, Issue 1 (2013), p. 110.

[118] *Ibid*, p. 111.

[119] SEC(2010)315, March 24, 2010: UE Recommendation from the Commission to the Council to authorize the opening of negotiations for an agreement between the European Union and the United States of America to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing.

agreement that, this time, involved the Parliament and considered its suggestions[120]. The new text required the Europol to evaluate the legitimacy of the requests of the USA and the guarantee of the privacy rights established in the American Privacy Act. Moreover, the Preamble to SWIFT-II contains a reference to fundamental rights and the right to privacy, ensuring that the EU and the USA are aware of:

"Article 6(2) of the Treaty on European Union on respect for fundamental rights, the right to privacy with regard to the processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union, the principles of proportionality and necessity concerning the right to private and family life, the respect for privacy, and the protection of personal data under Article 8(2) of the European Convention on the Protection of Human Rights and Fundamental Freedoms, Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union"[121].

The revised SWIFT Agreement (SWIFT-II) was approved by the Parliament in July and entered into force on August 1st, 2010, replacing the SWIFT Interim Agreement. A second rejection by the Parliament was very unlikely because of the importance for the EU to become a significant partner for the USA in the field of counterterrorism, and due to the "Parliament's ambition to be seen as a 'responsible' partner by the US and other EU institutions, in a context where many member states believed that such a gap in the TFTP system would be detrimental to their security"[122]. Still, SWIFT II was criticized by the European Data Protection Board and by part of the civil society[123].

The TFTP is a concrete example of the excessive monitoring activities of the United States, which have always been a cause of concern in the European Union and negatively affected bilateral relations. The Program, moreover, shows the different approaches of the US and the EU towards the value of privacy. The level of surveillance imposed by the TFTP did not raise as many concerns in the US as it did in the EU. Instead, the Program enjoyed the support and consensus of the American institutions. Indeed, following the leak on the secret Program, the House of Representatives passed Resolution H.R.895 on June 29, 2006, in which considered the TFTP as lawful, condemned the revelation of classified information[124]. By contrast, the European Union had hard times in balancing the values of privacy and security in order to reach to a final

[120] M. Romaniello, p. 112.
[121] (Second) Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Preamble. Text available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2010.195.01.0003.01.ENG&toc=OJ:L:2010:195:TOC#L_2010195EN.01000501.
[122] Ferreira-Perreira, Laura C. and Martins, Bruno Oliveira, *The European Union's Fight Against Terrorism: The CFSP and Beyond* (Routledge, 2014), p. 31.
[123] Sylvia Kierkegaard, "US War on terror EU swift(ly) signs blank cheque on EU data", *Computer Law & Security Law Review*, No. 27 (2011), pp. 451-464.
[124] U.S. House of Representatives, *The Terror Finance Tracking Program: hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services* , 109th Congress, Second Session, July 11, 2006 (Washington: U.S. G.P.O., 2007), p.68.

agreement due to the high status of the right of privacy in Europe, and the resulting division within the European Union during the negotiations for the SWIFT Agreement. However, while the SWIFT-II Agreement with the EU highlights the multilateral approach that characterized the Obama administration, the TFTP, is proof of the unilateralism of Bush administration, because of the secrecy that characterized the US initiative in spite of the existence of international means to cooperate against terrorism[125].

The study of the cooperation between the European Union and the United States against the terrorist threat is enlightening for the purpose of this thesis. Even though they are both democracies, uphold fundamental rights and the shared value of security, the relationship between privacy and security is completely different in the two realities. The next chapter will present the legal frameworks on the protection of privacy and personal data of the United States and the European Union, highlighting the differences between the systems and showing how privacy affects their cooperation on information sharing as a counterterrorist strategy. The PNR case will be analyzed, as it exemplifies the compatibility problem between privacy and security.

[125] Eric A. Caprioli, "Violation des règles propres aux données à caractère personnel et réseau SWIFT", *Revue de Droit bancaire et financier*, No. 1 (January 2007), p.34.

Chapter IV - THE VALUE OF PRIVACY IN THE EU AND THE US

Even though the European Union and the United States uphold the same values and cooperate for security purposes while trying to combat the menace of terrorism, their cooperation is not unproblematic. Indeed, as it will be further explained in this chapter, the European Union and the United States do not protect privacy in the same way. Their different approaches to the right to privacy have a relevant effect on their cooperation on information sharing for security reasons. The next paragraphs will analyze the legal frameworks for privacy and personal data protection of these two international actors, highlighting the differences between the two regimes of protection, and will provide a concrete example of how the two different levels of privacy obstacle bilateral negotiations on information sharing.

4.1 Legal frameworks: privacy and data protection

As deeply examined later in this section, the United States and the European Union have adopted very different legal approaches that, until recent developments, had often put them in contrast. Indeed, the European Union aims at strictly regulating the processing of personal data and their improper use. By contrast, the United States allows for extensive collection and storage of personal data. The huge difference between the two legislations is the cause of the disagreement in the context of the regulation of the cross-border flow of data, which is well exemplified by the PNR Agreement case that will be later presented in this chapter.

4.1.1 Privacy in the European Union

In the European Union, the origin of the notion of privacy finds its grounds in history. The fact that the Member States of the Union experienced dictatorships certainly had a strong influence on the development of a strict regime of regulation of the personal sphere. In fact, the manipulation of personal data

for political aims to enact repressive policies was common. A remarkable example is the promulgation of the racial laws in Italy during the fascist regime[126].

In Europe, the first instance of a regime that safeguarded privacy dates back to 1950, when the European Convention for the Protection of Human Rights and Fundamental Freedom was adopted. Article 8 regulating privacy, however, is very general.

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[127]

The case law of the European Court of Human Rights (ECtHR) regulates the legitimacy of state interference in the personal realm, considering that the second paragraph of Art.8 lists the necessary conditions that could be used to limit the privacy of an individual for the general interests of a democratic society. The requirement of necessity in a democratic society is crucial and has been clarified by the ECHR. According to the Court, states, in their activity to protect democracy, do not have an absolute power to monitor the individuals under their jurisdictions, especially if the measures that are adopted for monitoring activities may disrupt the democratic values they want to protect.[128] This decision is particularly important because it really highlights the regulatory approach to counterterrorism of the European Union that was discussed in the second chapter of this thesis. Indeed, the ECtHR identified the violation of the Convention by a law against terrorism and espionage of the Federal Republic of Germany, that provided for limitation to the secrecy of correspondence and telecommunication. Moreover, a series of judgments of the ECtHR resulted in "changes to the law to protect UK citizens against arbitrary or disproportionate intrusion into their privacy through the use of various forms of surveillance"[129], starting with Malone v. UK[130].

Although the EU is not bound by the ECtHR's decisions, the EU has a special consideration of the rulings of the ECtHR, as it considers them as establishing guidelines for the respect of human rights. The EU, indeed, is bound to access the European Convention for the Protection of Human Rights and Fundamental Freedoms

[126] Susan Zuccotti, "The Italian Racial Laws, 1938-1943: A Reevaluation", in "The Fate of the European Jews, 1939-1945: Continuity or Contingency?", Jonathan Frankel ed., Studies in Contemporary Jewry, Vol. XIII (Oxford University Press: 1998), p. 135.
[127] European Convention of Human Rights and Fundamental Freedoms, Art 8.
[128] Klass and others v. Federal Republic of Germany, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, September 6, 1978.
[129] Alice Donald, Jane Gordon and Philip Leach, "The UK and the European Court of Human Rights", *Equality and Human Rights Commission Research Series*, No. 83 (2012), p.67.
[130] Malone v. UK, No. 8691/79, April 26, 1985. See also: Halford v. UK, No. 20605/92, June 25, 1997.

(ECHR) after the entry into force of the Treaty of Lisbon in 2009, thus now bound by article 6 of the Treaty of the European Union:

"The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties".

Moreover, the EU Charter of Fundamental Rights protects the ECHR regime in art. 53, which states:

"Nothing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognised, in their respective fields of application, by Union law and international law and by international agreements to which the Union, the Community or all the Member States are party, including the European Convention for the Protection of Human Rights and Fundamental Freedoms, and by the Member States' constitutions".

The aim of article 53 of the EU Charter is to ensure that the level of protection of rights currently reached at international level is also protected. In addition, the access of the EU to the regime of the ECHR is allowed by Protocol n.14 of the Convention.

This system is very complex, and causes contrasts between the ECtHR and the ECJ. Indeed, after the accession there will be the external monitoring activity of the ECtHR. Moreover, the fact that EU member states will be bound by the Convention and liable for violations of the Convention within their jurisdiction, even if the violation is due to application of EU provisions, might endanger the primacy and autonomy of EU law. In order to avoid contrasts, the ECJ has tried to treat the Convention as part of EU law, but issues remain. For instance, in 2013, the Council of Europe and the EU negotiations finalized an agreement on the accession of the EU to the Convention regime. However, in 2014 the ECJ manifested its disagreement[131].

In 1981, the Council of Europe also stipulated the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention N.108), which has the aim to conciliate the need for free circulation of information deriving from personal data and the need for privacy.[132] The Convention lists the principles to be followed in the processing of personal data, as the proportionality principle (the proportion between the content of the information and the goal to be achieved), the correct use of sensitive information, the adoption of technical safety measures. This Convention is particularly important for the equivalence principle, which requires two states to ensure the same level of guarantees and privacy protection when they want to share information. Importantly, the Convention "is the only binding

[131] Opinion 2/13 of the ECJ, December 18, 2014.
[132] No. 108. Convention for the Protection of Individuals with regard to Automatic. Processing of Personal Data. Strasbourg, 28.I.1981 Art.1.

multilateral instrument in the area of data protection"[133]. Even though "the EU is not a party to the Convention, the Commission enjoys observer status"[134], and all the EU MS are members of the Convention. Thus, Convention N.108 plays an important role in the European Union in the context of privacy protection.

In 1995, the Data Protection Directive N. 95/46/CE was adopted by the European Parliament and the Council. Originally, the Directive was conceived to build a common standard for the safeguard of personal data. The Directive came before the Nice Charter (Charter of Fundamental Rights of the European Union), and notably the principles of the Directive were adopted by the Charter[135]. Thus, both the ECHR (Art. 8) and the Charter of Fundamental Rights of the European Union (Articles 7, 8) recognize the protection of privacy and personal data as human rights. The legal framework for privacy included also the e-Privacy Directive 2002/58/EC, which regulated the use of and access to personal data of natural persons in the electronic communications sector, and established a central supervising and consulting body for the protection of privacy and personal data, namely the European Data Protection Supervisor (EDPS). The e-Privacy Directive was amended in 2006 by the so-called Data Retention Directive (Directive 2006/24/EC), which was conceived to harmonize the rules for the retention of personal data by electronic communications providers, in order to facilitate the investigation and prosecution of serious crimes. However, as it will be further analyzed in the paragraph dedicated to the role of the courts in the protection of privacy rights (Section 4.1.3), the Data Retention Directive was declared invalid by the European Court of Justice in 2014[136], for violating Articles 7 and 8 of the Charter.

In 2012, the European Commission announced the possibility of reforming the European legislation concerning privacy. The aims were strengthening the protection of personal data as a fundamental right and creating new opportunities for the digital market. The reasons behind the reform of the laws on privacy were numerous. First of all, the Data Protection Directive had been approved in 1995 and since then there have been crucial transformations of the IT sector. Secondly, the number of people that could have access to the Net had exponentially increased, causing a dramatic increase in the circulation of data. Thirdly, the emergence of a whole variety of social networks required the massive amount of information created to be secured. Fourthly, the European Union had the necessity to safeguard privacy at international level, in the context of the opening of negotiations on information sharing agreements with third parties. All these motivations brought to the reform of the legal framework for the protection of privacy, which now includes:

[133] "Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalized World", *European Commission*, January 10, 2017, pp.11-12.
[134] COM(2012)679/F2, Brussels, November 16, 2012.
[135] Lucia Miglietti, "Profili storico-comparativi del diritto alla privacy", *Diritti Comparati*, December 4, 2014. Available at: http://www.diritticomparati.it/2014/12/profili-storico-comparativi-del-diritto-alla-privacy.html.
[136] Joined cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others EU:C:2014:238.

- Regulation (EU) 2016/679, which replaces Directive N. 95/46/CE on data protection and it will be directly applied in all the EU member states by 25 May 2018;[137]
- Data Protection Officer introduced by the above Regulation;
- Directive (EU) 2016/680 on the use of data by the authorities with the aim of prevention, investigation and criminalizing crimes or executing penal sanctions, which replaces Decision 2008/977/GAI of the Council, and will have to be incorporated into national law by May 2018;[138]

All this provides the EU with "the most protective regional framework in the field of data protection"[139].

4.1.2 Privacy in the United States

In the United States, the concept of privacy is very broad and there is no universally accepted legal definition. The protection of privacy is essentially based on rulings of the US Supreme Court, very specific federal laws and on a system of self-regulation[140]. However, this should not suggest that privacy is not seen as a fundamental value in the United States. On the contrary, the United States contributed to the elaboration of international general guidelines on the protection of privacy.

Unlike the European Union, where the right to privacy enjoys the status of fundamental right, the US Constitution does not contain any express reference to privacy. Nevertheless, the Amendments to the Constitution contain references that can be associated with various aspects of privacy, notably the Fourth Amendment that protects individuals and their properties against unreasonable searches:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"[141]

"American courts have articulated clear protections under the Fourth Amendment"[142], as well as under other amendments, through their decisions. Indeed, privacy related to intimacy, abortion[143] and marriage has been

[137] See also Regulation (EU) 2016/679. Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
[138] See also Directive (EU) 2016/680. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG.
[139] "Information society, privacy and data protection", *European Union Agency for Fundamental Rights*. Avaiable at: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection:
[140] Marsha Cope Huie; Stephen F. Laribee; Stephen D. Hogan, "The right to privacy in personal data: the EU prods the US and controversy continues", *Tulsa Journal of Comparative and International Law,* Vol. IX, Issue 2 (Spring 2002) p.79.
[141] See also http://constitutionus.com/.
[142] Patricia Boling, "Deprived, Protected, Empowered", *Privacy in America* , eds.William Aspray, and Philip Doty (Lanham, UK: The Scarecrow Press, Incs, 2011), p. 4.

protected thanks to the Supreme Court interpretation of the Fourteenth Amendment[144]. For instance, in Lawrence v. Texas[145], the US Supreme Court stroke down the Texan antisodomy law on privacy grounds. Furthermore, the Fifth Amendment protects people against self-incrimination[146] (no one can be obliged to testify against himself or herself), which "serves as a basis for a type of privacy protection, especially psychological privacy"[147]. The Supreme Court has also expanded the scope and protection of privacy with many judgments, as in Whalen v. Roe[148], recognizing the right to information privacy, or in Eisenstadt v. Baird[149], stressing that privacy is a right of the individual[150]. Moreover, even though the right to privacy is not expressly referred to in the Constitution, the Supreme Court of the US recognized the possibility for the federal states to guarantee higher levels of protection of privacy in the case Katz v. United States[151]. As a consequence, many states started to develop their own legislations on privacy. However, this resulted in a very uneven framework for the protection of privacy, since the level of privacy protection may greatly vary between different states and significantly differ from the federal level.

The only instrument at federal level that offers privacy protection and regulates the collection and use of personal data is the 1974 Privacy Act. The Act codifies the necessary principles for the collection and analysis of personal data, among which transparency, individual participation, limited collection of data through appropriate means, and for the right scope. The Act, however, is limited to certain specific fields[152]. Moreover, until 2015, the Act applied only to US citizen, permanent residents, and foreign visitors. As it will be explained later, the 2015 Judicial Redress Bill[153], which extended the protection to EU citizens, marked a crucial shift in the bilateral negotiations on information sharing between the United States and the European Union.

Considerations about the level of privacy in the United States must follow only after the analysis of other factors that influence the protection of privacy. The US has no central supervising body, but rather various monitoring authorities, like the Government Accountability Office (GAO) and the Department of Homeland Security (DHS) Privacy Office. However, privacy authorities have been criticized for not being

---

[143] See: *Griswold v. Connecticut* 381 U.S. 479 (1965) (protecting the right to prescribe or use contraceptives); *Roe v. Wade* 410 U.S. 113 (1973) (protecting the right to abortion on grounds of privacy).
[144] *Ibid*, p. 6.
[145] *Lawrence v. Texas*, 539 U.S. 558 (2003).
[146] P. Boling, p. 230.
[147] Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy (University of North Caroline Press: 2009), p. 38.
[148] 429 U.S. 589 (1977).
[149] 405 U.S. 438 (1972).
[150] *Ibid*, p.39.
[151] *Katz v. United States*, 389 U.S. 347 (1967).
[152] "National Strategy for Information Sharing: Successes and Challenges In Improving Terrorism-Related Information Sharing" *Nationwide Sar Initiative* (October 2007). Available at: https://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf.
[153] Jourová, Věra "The future of U.S.-EU data transfer arrangements at the Brookings Institution" *European Commission Press Release Database* (Speech/156104). Available at: http://europa.eu/rapid/press-release_SPEECH-15-6104_en.htm.

enough independent from the government. Consequently, the US lacks the sufficient oversight mechanisms that are necessary to ensure an effective protection of privacy[154].

Not only does the US lack a substantial level of privacy protection at federal level, but also is not able to protect privacy rights that are guaranteed at international level, notably by the International Covenant on Civil and Political Rights (ICCPR). Though the US is a signatory state of the ICCPR, the United Nations Human Rights Committee has rated the US low on privacy protection[155]. Indeed, "the US (fails) to establish meaningful judicial oversight of its surveillance operations, adequate limits on data retention, and meaningful access to remedies for privacy violations"[156].

Although the problem of privacy is particularly felt in the United States, poor protection of privacy has enabled the US government to easily initiate negotiations for agreements on information sharing with the European Union. However, considering the relevance that the EU attribute to the right to privacy, the level of privacy protection of the US is considered as being inadequate by the European Union. Indeed, in order to speed up the agreement making process on information sharing, as we will see later on in this chapter, the US was forced to agree with the European Union on higher level of privacy protection (e.g. through the Judicial Redress Bill, and EU-US Privacy Shield[157]).The aim of the next section is to further analyze the protection of privacy in the context of a developing IT technology and of an increasing terrorist threat. The goal is to provide the reader with additional knowledge and information about the difference between the United States and the European Union concerning the actual protection of the right to privacy.

4.1.3 Data retention violations after 9/11 and the role of the courts in protecting privacy

As anticipated in the second chapter, regulation and oversight for the management of data are needed in order to guarantee the fragile balance between security and privacy within democracies. For these monitoring purposes, courts, judges and data protection commissioners play an important role. This section examines the activity and efficiency of courts in the United States and the European Union in performing their role of supervisory bodies for the protection of privacy.

---

[154] Hiroyuki Tanaka, Rocco Bellanova, Susan Ginsburg and Paul De Hert, *Transatlantic Information Sharing: At a Crossroads* (Washington, DC: Migration Policy Institute, 2010), p.30.

[155] "Follow-up to Concluding Observations", *Center for Civil and Political Rights.* Available at: http://ccprcentre.org/page/114th-session-in-brief/follow-up-to-concluding-observations?/114-session-follow-up-concluding-observation/.

[156] "U.S. Receives Low Grades on Privacy and Surveillance from UN Committee", *Brennan Center for Justice,* July 18, 2015. Available at: https://www.brennancenter.org/press-release/us-receives-low-grades-privacy-and-surveillance-un-committee.

[157] Mike Snider and Elizabeth Weise, "EU, U.S. agree on data sharing pact*", USA Today*, July 12, 2016. Available at: http://www.usatoday.com/story/tech/news/2016/07/12/eu-us-agree-privacy-shield-data-rules/86980774/.

4.1.3.1 The European Union

Judicial activities are crucial for protecting privacy in the European Union, both at European and at Member State level. After the terrorist attacks of 2004 in Madrid and of 2005 in London, the European Parliament adopted the 2006/24/CE Directive on Data Retention, concerning the retention of data by communication services. In 2009, the European Court of Justice confirmed that the Directive complied with the competences of the European Union and its legal basis, but it was not involved in any judgment regarding its compliance with human rights[158]. The issue of the compliance with fundamental rights was raised at Member State level, notably by the Irish High Court and the German Constitutional Court three years later, and by the Austrian Constitutional Court in 2012[159]. Thanks to the concerns expressed by the MS, the Court finally reached a decision in 2014. In the Digital Rights[160] judgment of April 2014, the Court found a violation of the proportional principle granted by Articles 7 and 8 of the Charter of Fundamental Rights, which refer to the general protection of data and privacy. In its previous judgment regarding the Directive, the Court had already found its legal basis in Art. 95 of the EC Treaty against the opinion of Ireland and the Slovak Republic[161]. The Court found that the retention of data is a correct means to fight terrorism. Nevertheless, in the 2014 judgment, it found that the Directive violated some necessary conditions: the unlimited scope, the variable timing of retention without any reference to the typology of retained data, the lack of oversight instruments, the insufficient protection of retained data and the generality of the Directive were not acceptable by the Court.[162]

The judgment of the ECJ has led to several problems within the EU. As it happens for any EU Directive, national legislators transposed the Directive on Data Retention into national legislation. However, when the European Directive was invalidated, national data retention legislations that had been previously put in place to implement the Directive were not invalidated. The current problem is that since the ECJ invalidated the Directive because of its violation of fundamental rights, it is not difficult to think that national laws that had been passed on the basis of that Directive are violating fundamental rights, in turn[163]. Consequently, a great number of cases against national data retention laws were brought before their national courts in order to assess whether their data retention regimes violate fundamental rights as

[158] Jürgen Kühling, and SonjaHeitzer, "Returning through the national back door? The future of data retention after the ECJ judgment on Directive 2006/24 in the UK and elsewhere", *European Law Review* (April, 2015), pp.263-278. Available at: https://ael.eui.eu/wp-content/uploads/sites/28/2015/04/Spaventa-08-Kuhling-Heitzer.pdf.

[159] See also: BVerfG, 1 BvR 256/08, 3 March 2010 (Germany); VfSlg 19.632/2012 (Austria).

[160] See also: Digital Rights Ireland (C-293/12) EU:C:2014:238.

[161] Ireland v. European Parliament, Council of the European Union, C-301/06, Grand Chamber, Judgment, February 10,2009.

[162] *Ibid.*

[163] Franziska Boehm, and Mark D. Cole, "Data Retention after the Judgment of the Court of Justice of the European Union" (June 30, 2014), p. 48. Available at: https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf.

interpreted by the ECJ in its judgment on Directive 2006[164]. Recently, the Advocate General Saugmandsgaard Øe (A.G.) gave his (nonbinding) opinion on two cases brought before the ECJ to judge the compatibility of the UK and the Swedish data retention laws with EU legislation[165]. According to the EU e-Privacy Directive, national legislation regulating the retention of data can be passed, and the A.G. clarified that this kind of legislation can be perfectly compatible with EU law, as long as it respects some safeguards. However, this position remains problematic[166]. Indeed, it is striking to notice that several national Constitutional Courts invalidated national legislation implementing the Directive requirements, as the Bulgarian Constitutional Court[167], the Belgian Constitutional Court[168], and the Slovenian Constitutional Court[169].

As Federico Fabbrini notices[170], there are many reasons behind the willingness of courts to intervene in the national sphere and rule on the protection of fundamental rights, despite the existence of national security needs. Especially in the case of the fight against terrorism, courts are more hesitant to intervene against political decisions, but as time passes the urgency behind the adoption of some policies loses its significance. As a consequence, courts may start to put limits to the executive and legislative branches and (find stronger arguments to remedy perceived limitations of human rights). Moreover, sometimes supranational and international courts are in a better position than national courts in defending human rights, because they are detached from the particular political environment of states. Additionally, "they are not subject to the cut-off application of secrecy claims (…) (and) are less constrained by procedural rules"[171].

As demonstrated, the European Court of Justice has a prominent role in defining the proper safeguards that are needed to retain data. Additionally, even national courts are playing a decisive role in the protection of privacy, as in the already mentioned examples of the Belgian, Bulgarian and Slovenian Constitutional Courts annulling the laws derived from the European Directive. A similar case happened in 2015 in the Netherlands, where the national Telecommunications Data Retention Act was first suspended and then repealed as a consequence of the ECJ judgment[172].

In the EU, the courts are intervening also by limiting the power of intelligent agencies in the processing of personal data for security purposes. An example is the decision of the European Court for

[164] *Ibid,* p.49.
[165] Advocate General's Opinion in Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for Home Department v Tom Watson and Others.
[166] Maria Tzanou, "The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance", *Modern Studies in European Law,* No. 71 (Hart Publishing, June 1, 2017), p. 103.
[167] Decision N. 2 Case 8/2014, March 12, 2015.
[168] Decision 84/20015, June 11, 2015.
[169] Decision of 3 July 2014, No. U-I-65/13-19.
[170] Federico Fabbrini, "The Interaction of Terrorism Laws with Human Rights", in *Routledge Handbook of Law and Terrorism*, eds. Genevieve Lennon, and Clive Walker (Abingdon, OX: Routledge, 2015), pp. 97-98
[171] *Ibid.*
[172] Stichting Privacy First et al. v. de Staat der Nederlanden, Case No. C/09/480009 / KG ZA 14/1575 (Mar. 11, 2015).

Human Rights, which in 2016 condemned a Hungarian anti-terrorism law of 2011 due to its too generic provisions on wiretapping procedures in the case Szabò v. Hungary[173]. In this case, the (Strasbourg) Court has highlighted the importance of respecting the legal principles regulating the processing of personal data and privacy (necessity, proportionality, scope and timing) even when national security is at stake[174].

Additionally, the European courts are very active in the protection of privacy against non-European actors' violations, thereby protecting European standards on privacy. For example, in October 2015, in Maximilliam Shrems v. Data Protection[175], the Court of Justice of the European Union invalidated the European Commission decision 2000/520/CE which had accepted the level of privacy protection granted by the United States in the Safe Harbor regime (now corrected by the Judicial Redress) because of the indiscriminate and massive collection of personal data belonging to European citizens by the American government for national security reasons.[176]

Moreover, the case of a proceeding started by the Belgian commissioner against Facebook[177] is just one example of the active role of data protection commissioners within the European Union. Thus, not only is the EU characterized by a incredibly strict legal framework for privacy, but also by a very strong system of oversight thanks to the activities of European and national courts and other supervisory bodies.

4.1.3.2 The United States

After the terrorist attacks to the Twin Towers, the Congress of the United States passed the PATRIOT Act (2001), which expanded the monitoring powers of the government for the sake of national security. The PATRIOT Act was able to do so by amending every law regulating privacy[178]. The Act was passed bypassing the system of committees, and it was approved thought large majorities both in the Senate and in the House of Representatives after limited discussions[179]. However, despite the introduction of the

[173] "La società sorvegliata", *Garante Privacy,* Atti del Convegno, January 8, 2016, p. 74. Available at: http://194.242.234.211/documents/10160/5312012/La+societ%C3%A0+sorvegliata+-+Atti+del+convegno+del+29+gennaio+2016.

[174] *Ibid,* p. 150.

[175] Case C-362/14.

[176] "The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid", Court of Justice of the European Union PRESS RELEASE No 117/15, Luxembourg, October 6, 2015. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

[177] See Belgian Commission for the Protection of Privacy v Facebook, Dutch Speaking Court of First Instance, Brussels, (November 9, 2015). Available at: https://www.privacycommission.be/en/news/judgment-facebook-case, accessed April 12, 2017.

[178] Robyn R. Mace, "Intelligence, Dataveillance, and Information Privacy", *Protecting Persons While Protecting the People*, eds. Cecilia S. Gal, Paul B. Kantor, and Michael E. Lesk (Springer, 2009), p.35.

[179] John Ip, "Terrorism laws and constitutional accountability", in Routledge Handbook of Law and Terrorism, Genevieve Lennon, and Clive Walker (eds), (Abingdon, OX: Routledge, 2015), p.102.

Inspector General for the Department of Justice (DOJ), a supervision body for the control of the NSLs, the FBI was repeatedly found guilty of violating the law[180]. From that moment on, the surveillance activities of the American Government have been a major concern, especially with regards to the protection of personal data and privacy guaranteed to the US citizens. For being highly criticized, several pieces of legislation were passed in order to properly regulate the procedures for accessing personal data and protecting privacy in general (1974 Privacy Act, 1987 Computer Security Act, etc). As far as criminal investigations are concerned, judges can issue orders that enables law enforcement authorities to monitor online communications in real time only if there are findings on a committed crime or on a crime that is being or is about to be committed. However, the major problem has been the incorrect interpretation of the PATRIOT Act by the government and its abuse of power. Additionally, concerning the access to stored data, the Electronic Communications Privacy Act (ECPA) does not even require a judicial approval.

The control that the United States has on its citizens is huge. Several times security agencies as the National Security Agency initiated secret programs for security purposes that had been discovered and denounced for their disregard of the law. At the end of 2005, the New York Times revealed the Terrorist Surveillance Program of the Bush administration, a secret program of wiretapping initiated with the aim to combat terrorism, which, however, was not authorized by any judicial authority. In 2006, the judgment of the federal judge Anna Diggs Taylor condemned the abuse of power of the Bush administration, and imposed the immediate interruption of the program for its violation of the First and Fourth Amendments of the USA Constitution.[181]

However, the first big scandal on mass surveillance in the United States occurred in 2013. The Foreign Intelligence Surveillance Court (FISC) interpreted the PATRIOT Act in a way that permitted the American telephone companies to let the NSA have access to all phone records[182]. In 2013, the former NSA contractor Edward Snowden revealed secret monitoring programs of the American government to the Guardian and the Washington Post. It was found that the NSA had started to access, store and analyze all the phone records associated with the phone numbers of any suspected terrorists. Thus, the PATRIOT Act is criticized for not properly protecting the privacy of people, since the collection of data is unlimited and indiscriminate[183]. In addition to the just mentioned NSA program, the leaks also revealed the NSA Prism Internet Surveillance Program[184]. According to the revelations, the NSA was obliging US companies as

[180] *Ibid*, p.106.
[181] "La società sorvegliata", *Garante Privacy,* Atti del Convegno January 8, 2016, pp. 47-48. Available at: http://194.242.234.211/documents/10160/5312012/La+societ%C3%A0+sorvegliata+-+Atti+del+convegno+del+29+gennaio+2016.
[182] 218 F. Supp. 2d 611 (US FISC 2002).
[183] Greg Nojeim, "When Metadata Becomes Megadata: What the Government Can Learn", *CDT*, June 17, 2013. Available at: https://cdt.org/blog/when-metadata-becomes-megadata-what-the-government-can-learn/.
[184] Alicia Parlapiano, "Comparing Two Secret Surveillance Programs", *The New York Times*, June 7, 2013. Available at: http://www.nytimes.com/interactive/2013/06/07/us/comparing-two-secret-surveillance-programs.html?_r=0.

Google and Facebook to grant access to their servers, in order to collect all kinds of online communications data. This program was based on the Foreign Intelligence Surveillance Act (FISA), and constituted an international scandal since the targets were mainly foreigners.

Particularly after the Snowden revelations, PEN International ("a non-political organization which holds Special Consultative Status at the UN and Associate Status at UNESCO"[185], constituted by writers and whose main aim is strengthening freedom of expression) has conducted many researches on the level of surveillance in several countries, noticing that anti-terrorist programs have been used to justify repression of human rights and even self-censorship of writers and journalists.[186] PEN International's opinion has been confirmed by the 2014 report of Freedom House about the decline in Internet freedom. According to the report, surveillance increased and repressive laws were passed all around the world. After the leak of news about the NSA spying operations, the United States' surveillance activities have been heavily criticized by the civil society but have also been a justification for other states to increase their level of surveillance[187]. Within the USA, the Congress had to pass legislation to protect the right to privacy, but the legislation merely confirmed and legalized the practice of surveillance. In spite of the recently passed legislation, in 2015 another leak of news revealed the NSA wiretapping of European leaders.

Mass surveillance increased in 2016 under the Trump administration. The Amendment of the Federal Rules of Criminal Procedures simplified the access to computers[188]. Moreover, the appointments that characterized the American administration may further endanger the current status of protection of privacy, since the new administration seems to prefer national security requirements and emergency exceptions over human rights protection needs. For instance, Mike Pompeo, appointed as the CIA head, and Jeff Sessions, the new Attorney General, have both criticized the 2015 FREEDOM Act for its impediments to the NSA activities and the ECPA.[189]

An additional issue in terms of violation of the right to privacy and surveillance concerns the use of anonymity on the net. Although in the United States there is no legal restriction on the use of anonymity,

[185] See also: http://www.pen-international.org/who-we-are/

[186] Sarah Clarke, "The Dissident Blog's Issue #17 – Digital Threats", *Pen International*, July 8, 2015. Available at: http://www.pen-international.org/07/2015/mass-surveillance-and-online-censorship-the-pen-international-prespective/.

[187] Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong, "Tightening the Net: Governments Expand Online Controls, Freedom on the Net (2014)", *Freedom House*, p. 878. Available at: https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf.

[188] Richard Hsu, "Government Surveillance Under a Trump Administration", *Shearman and Sterling*, December 19, 2016. Available at: http://www.shearman.com/en/newsinsights/publications/2016/12/govr-surveillance-under-a-trump-administration.

[189] Richard Hsu, Government Surveillance Under a Trump Administration, *Shearman and Sterling*, December 19, 2016. Available at: http://www.shearman.com/en/newsinsights/publications/2016/12/govr-surveillance-under-a-trump-administration.

"there is evidence to suggest that the intelligence community in the U.S. has been working to undermine the security of anonymizing tools"[190].

All the above factors demonstrate the fact that the USA falls short of an adequate system of oversight of the intelligence[191], which has been criticized for recurring violations of the Constitution. Thus, as already pointed out in the second chapter, transparency of security programs, institutional accountability and oversight of judicial authorities are fundamental to safeguard citizens' rights and their privacy.

The numerous violations of privacy rights in the USA is inconsistent with the great influence of the Supreme Court on government activities. The Supreme Court is regulated by the Constitution and by the US Code (USC). Its immense power was clear in the Marbury v. Madison[192] case, which for the first time found a federal law unconstitutional and introduced the function of judicial review of the Supreme Court, as well as any other court. Additionally, the Supreme Court proclaimed its supremacy in the interpretation of the Constitution in Cooper v. Aaron[193]. However, the Supreme Court, as well as the American judiciary branch in general, found themselves in a state of enduring contrast with the executive. A striking example is the case of Yaser Hamdi, an American who was captured in Afghanistan and arrested for his alleged association with the Talibans. When he filed a petition for habeas corpus, the Supreme Court decided that the challenge had its legal basis in the Fifth Amendment[194]. In a subsequent case (Rasul v. Bush), the Supreme Court also recognized that "federal courts (had) jurisdiction to hear habeas corpus from foreign nationals captured outside the United States"[195]. However, the Military Commissions Act of 2006 passed by the Congress decided that the federal courts could not hear any more habeas corpus petitions filed by enemy combatants. The Act of 2006 was an attempt by the US Congress to bypass the decision of the Supreme Court for the enemy combatants detained in the military prison of Guantanamo. The Supreme Court declared the Act unconstitutional in the Boumediene case of 2008[196], "making clear once and for all the principle that procedural guarantees applied as far as Guantanamo's detainees were concerned"[197]. Even though the US Supreme Court finally succeeded, these cases exemplify the contrast between the Congress and the Supreme Court concerning the respect of human rights and the abuses of the US government.

---

[190] Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong, "Tightening the Net: Governments Expand Online Controls, Freedom on the Net (2014)", *Freedom House*, p. 889. Available at: https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf.

[191] *Ibid,* p. 6.

[192] Marbury v. Madison, 5 U.S. (1 Cranch) 137 (1803).

[193] Cooper v. Aaron, 358 U.S. 1 (1958).

[194] Hamdi et al v. Rumsfeld et al, 542 US 507 (2004).

[195] Larry J. Siegel, *Criminology: Theories, Patterns, and Typologies* (Cengage Learning, 2016), p.402. See also: Rasul v. Bush (03-334) 542 U.S. 466 (2004).

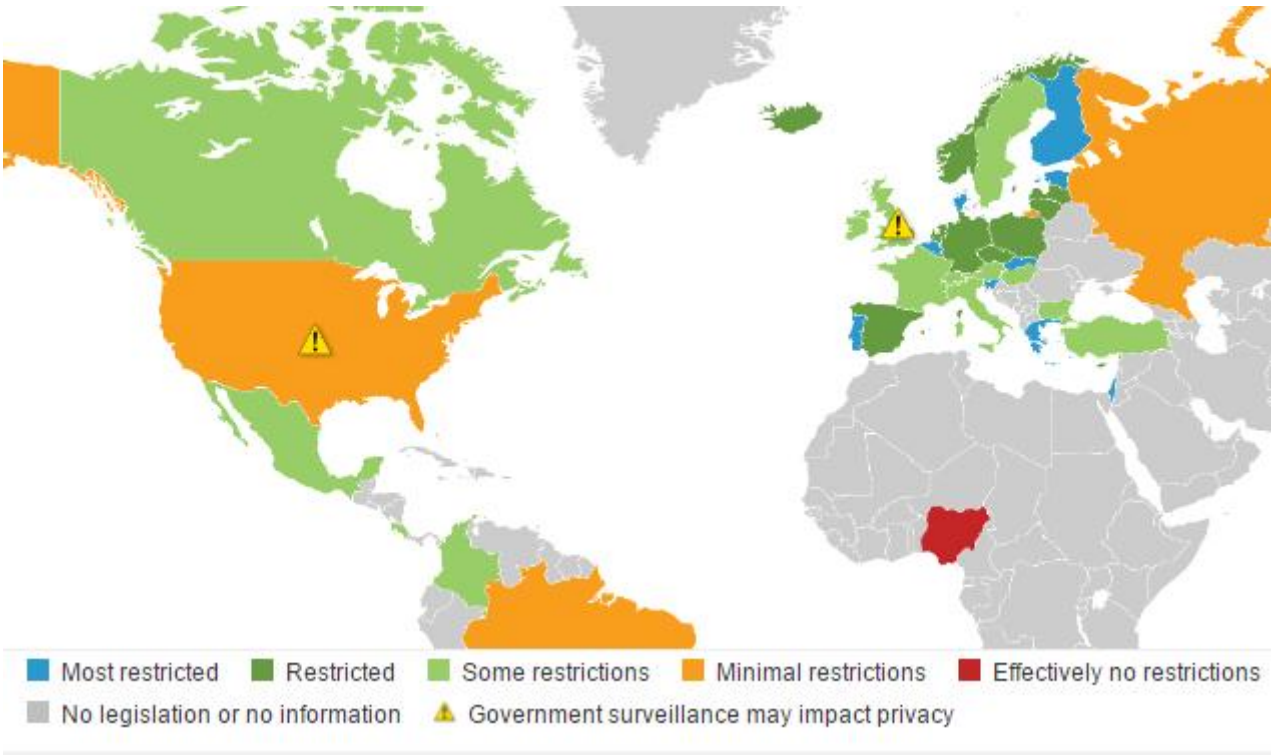
[196] Boumediene v. Bush, 553 US 723 (2008).

[197] Federico Fabbrini, "The Interaction of Terrorism Laws with Human Rights", in *Routledge Handbook of Law and Terrorism,* eds. Genevieve Lennon and Clive Walker (Abingdon, OX: Routledge, 2015), p. 96.

4.1.4 Differences between levels of privacy

After the comparison of the legal frameworks of the US and the EU concerning the protection of privacy, it is evident that the levels of privacy of the two actors are certainly different. Firstly, although privacy finds constitutional legitimacy in both the European Union and the United States, in the USA the creation of protections on grounds of privacy rests within the jurisprudence of the US Supreme Court. Secondly, the legislation of the EU treats the right to privacy as a general right, protecting all the categories that may fall within this right, notably the category of personal data. Instead, the USA have a sectorial approach towards the right to privacy, so its protection is not as extensive as the protection granted in the EU. Thirdly, in the European Union the courts perform a much more active role with respect to the United States as supervisory bodies. Fourthly, abuses of power and violations of the protection of personal data are very common in the United States. A glance of the different levels of privacy protection can be noticed in Table 1.

Table 1. Privacy and data protection by country (2015)



Source: Forrester Research[198]

[198] "Privacy and data protection by country", *Forrester Research*. Available at: http://heatmap.forrestertools.com/

The Table shows that European countries are among the most restrictive ones in terms of the legal protection of privacy and personal data. Thus, the level of regulation of the rights to privacy and personal data is higher than in the United States, where "minimal legal restrictions" means that privacy is poorly regulated. Additionally, as already mentioned in previous paragraphs, the government surveillance impacts negatively on the protection of the right to privacy. Remarkably, the difference between the levels of protection of privacy in the US and the EU has slowed down the negotiations of agreements involving the right to privacy, as in the cases of the TFTP and PNR agreements.

4.2 The European Union struggle between privacy and security needs

The privacy concerns associated with information gathering has not prevented the European Union from developing internal databases for sharing information within the Union itself in the pursuit of security. An example is the Schengen Information System. Nor has this problem prevented the European Union, in performing its role as international actor, from concluding agreements on information sharing with third parties. However, privacy concerns influence the European Union propensity to accept international agreements that allow flows of information outside the boundaries of the EU.

The problem is that, on the one hand, privacy is a fundamental right, but on the other hand, many EU Member States are experiencing frequent terrorist attacks and the resulting profound fear of terrorism is influencing the opinion of the European population on the possibility to restrict fundamental rights in order to fight terrorism and organized crime. Following the terrorist attacks that involved some European states, claims for the share of more information have been raised, especially in the light of Schengen, which allows terrorists to move freely within the EU countries in the Schengen area. As a French parliamentary report in 2016 affirmed, the problem is not the existence of Schengen, but the poor coordination and share of information between intelligence forces, and the fact that intelligence agencies are not taking advantage of the potential tools that Shengen offers for security purposes[199]. However, the recent involvement of the European Union on issues regarding information sharing has led to many worries concerning the protection of privacy of EU citizens.

Indeed, more than half of the EU citizens observed that their fundamental rights and freedoms have been restricted due to the increasing engagement in the fight against terrorism. The percentage of citizens

[199] Francois-Noel Buffet (au nom de la commission d'enquête), "Circuler en sécurité en Europe: renforcer Schengen", Rapport No. 484 (2016-2017), March 29, 2017.

that believe their rights have been limited has increased by 5% with respect to 2011.[200] Thus, new security needs due especially to the escalation of terrorism have negatively affected the freedoms of EU citizens. However, concerning these needs, people tend to rely more on the activities of the national police forces and judicial branch, rather than on the activities of the European Union.[201] Thus, European institutions are perceived as being much more distant from citizens with respect to national institutions. As a consequence, it is more difficult for Member States to let the EU take decisions on privacy and security that could affect them. In the light of the 2013 Snowden revelations, for example, many states have used national security justifications to prevent the EU from intervening more in the management of counterterrorism through the share of information.[202] Though its role in the fight against terrorism is not seen as crucial as the role of national bodies, the European Union is continuing to engage in more and more negotiations with third parties to regulate the exchange of information for security purposes. However, in the light of the increased concerns regarding the negative impact of new security needs on privacy, the European Union is adopting a very specific strategy. It is no coincidence that the European Union has recently modified its legal framework regulating privacy (Section 4.1.1). Rather, the evolution of the legislation on the protection of privacy has a logic. The changes seem to be dictated by foreign policy choices and the desire to export the European standards on privacy to the international community. For example, the SWIFT Agreement that was previously analyzed was criticized as an European attempt to export its standards[203]. This consideration finds support in the adoption of the Stockholm Programme[204]. As far as fundamental rights are concerned, one of the objectives of the Programme is that "EU citizens must be able to exercise these rights within as well as outside the EU, while knowing that their privacy is respected, especially in terms of protection of personal data."[205] As for privacy, moreover, the European Union should promote to other states the application of its standards of protection of personal data, especially Convention N. 108, as well as the membership to the Convention. Indeed, as the Vice-President of the EU's Justice Commission said referring to the participation of the Commission to the negotiations with the Council of Europe on the Convention in 2012, the EU is "setting new and higher standards for data protection in the EU. But in this brave new digital age, data knows no national borders – these negotiations are an opportunity to build a new gold standard of

[200] "Europeans' attitudes towards security", *Special Eurobarometer 432* (April, 2015), p.12. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_432_sum_en.pdf.
[201] *Ibid,* p. 10.
[202] Didier Bigo, Sergio Carrera, Elspeth Guild and Valsamis Mitsilegas, "The EU and the 2016 Terrorist Attacks in Brussels: Better instead of more information sharing", *CEPS Commentary*, April 6, 2016. Available at: https://www.ceps.eu/publications/eu-and-2016-brussels-terrorist-attacks-better-instead-more-information-sharing.
[203] Justin Santolli, "The Terrorist Finance Tracking Program: Illuminating the shortcomings of the European Union's antiquated data protection directive", *The George Washington International Law Review,* Vol. XL, No. 2 (2008), p. 563. Available at: http://docs.law.gwu.edu/stdg/gwilr/PDFs/40-2/40-2-6-Santolli.pdf.
[204] "The Stockholm Programme", *Eur-Lex*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Ajl0034, accessed April 13, 2017.
[205] *Ibid.*

data protection across the globe"[206]. This view has been confirmed by the European Justice Commissioner Věra Jourová in a press release about new proposals by the European Commission of legislation aiming to update the current regulation concerning electronic communications. She affirmed that the Commission is currently elaborating a strategy regarding the international sharing of information and the promotion of European standards on data protection.[207]

As this dissertation will later discuss, the EU-USA PNR Agreement is also an example of the European struggle concerning the contrast between security and privacy. The literature on risk-perceptions suggests that in the aftermath of a terrorist attack, people's fears condition the authorities to adopt emergency policies and new legislation to prevent similar tragedies[208]. Those resolutions may be so extreme that could lead to a violation of fundamental law. The courts' intervention to restrain the legislative and executive branches from going too far, may actually be in contrast with the necessities of people, who do not feel protected. Whether it is right or wrong to let the public opinion influence political decisions and even prevail over the power of courts, it is true that people's perception of threats and their opinion influence the actions of a government[209]. Consensus and public opinion are among the main instruments for the exercise of popular sovereignty in a democracy. However, it is fundamental to not allow states to use fears for increasing control and monitoring activities. After the recent terrorist attacks in the European Union, the fear of terrorism is felt so deeply in its Member States that the tight grip of the government on privacy is evidently loosening, resulting in many worries. In 2015, a Eurobarometer survey showed that 49% of European citizens consider terrorism as the main threat in the EU, followed by the fear of economic crisis, religious extremism and organized crime.[210] The percentage concerning the fear of terrorism and religious extremism sharply increased since 2011, when only 33% of EU citizens regarded terrorism as a main source of insecurity, and only 6% of them were worried about extremism.[211] Therefore, dynamics of fears have changed throughout time, and the different percentages have influenced the choices taken on the management of privacy and security at the European Union level. Finding a balance between privacy and security is very difficult, especially when a new menace steps into the game and modifies the public opinion

[206] "Commission to renegotiate Council of Europe Data Protection Convention on behalf of EU", Brussels, November 19, 2012. Available at: http://europa.eu/rapid/press-release_MEMO-12-877_it.htm.
[207] "Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions", *European Commission Press Release* (Brussels: January 10, 2017) Available at: http://europa.eu/rapid/press-release_IP-17-16_en.htm.
[208] Victor V. Ramraj, Michael Hor, and Kent Roach, *Global Anti-Terrorism Law and Policy* (Cambridge University Press, 2005), p.6.
[209] See: Paul Slovic, "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield", *Risk Analysis*, Vol. XIX, Issue 4 (August, 1999) pp. 689-701; Lennart Sjoberg, "Political decisions and public risk perception", *Reliability Engineering & System Safety*, Vol. LXXII, Issue 2 (May, 2001), pp. 115-123.
[210] "Europeans' attitudes towards security", *Special Eurobarometer 432* (April, 2015), p. 6. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_432_sum_en.pdf.
[211] *Ibid.*

influencing the activities and choices of a state on the transfer of more attention and resources to one value rather than to the other one.

The following paragraph will analyze the case of the EU-USA PNR Agreement, which embodies the struggle of the European Union to find a balance between privacy and security and the contrasts between the European Union and the United States to reach a final decision due to their different approaches to security and privacy.

4.3 The roles played by privacy and security in the PNR case

Until now, one of the main instruments of the European Union for the regulation of personal data has been Directive 95/46/CE. Being the Directive a unitary instrument for the general protection of data, the case of the European Union is far from the situation in the United States, where the approach towards the protection of privacy is fragmented and sectorial. A crucial part of the Directive concerns the regulation of the outflow of data towards other countries outside the Union. When non-EU countries do not offer a proper level of privacy protection, the outflow of personal data is prohibited. Thus, while the European Union's strict regime guarantees an effective regulation and protection of privacy, it also constitutes a serious barrier for the development of negotiations on information sharing with other international actors. The EU-US Passenger Name Record (PNR) is an agreement that embodies the difficulty of the Union in reaching a final decision on the exchange of information due to privacy concerns.

The PNR is part of the European counterterrorism strategy to protect its citizens and reduce the vulnerability to possible terrorist attacks[212]. The expression Passenger Name Record (PNR) refers to personal data collected by airline companies following the booking of a ticket. After 9/11, the United States introduced a set of regulations that obliged airline companies to share the PNR information from all the planes departing from, in transit, or landing on the American soil with customs authorities. Thus, these disposition involved all the European airline companies that were subject to the European Directive 95/46/EC at the same time. As anyone can imagine, this situation was very inconvenient for the European companies involved. Indeed, under the European Directive, the transfer of PNR data constituted an outflow of data towards a third party. As previously mentioned, for these situations the European Directive did not allow the transfer of data towards countries outside the Union that couldn't guarantee the same level of

[212] "Lotta dell'UE al terrorismo", *Consilium*. Available at: http://www.consilium.europa.eu/it/policies/fight-against-terrorism/, accessed April 14, 2017.

protection of privacy. That marked the beginning of the controversy between the European Union and the United States. On the one side, the European Union wanted to ensure the protection of personal data of its citizens and the respect of national laws that had implemented the Directive. On the other side, even though the United States allowed for a delay of its new legislation about the PNR data to the month of March 2003, it provided that from March airline companies that couldn't respect the American legislation would have to be sanctioned. Thus, in 2003 the European Commission elaborated an interim agreement[213] which, however, allowed the EU Member States to disregard Directive 96/45/EC. Clearly, this situation raised many concerns regarding privacy, and the European Parliament strongly criticized the interim agreement[214].

In 2004 the first PNR Agreement was agreed upon by the Commission. Yet again, it was opposed and criticized by the Parliament and the civil society. The Parliament filed two complaints before the Court of Justice against the decision of adequacy of the Commission and the decision of the Council to conclude the agreement. In 2006 the Court agreed with the Parliament[215]. The Commission reacted asking the permission to the Council to open new negotiations with the United States. A temporary agreement was concluded at the end of 2006, but it was criticized for being even more invasive of the right to privacy. As the expiration date of the temporary agreement approached, the Commission opened again negotiations with the American Department of Homeland Security and reached a settlement in July 23, 2007. Once again, the second PNR Agreement was criticized for violating the necessary requirements for the transfer of data outside the European Union. The deadline for the second agreement was 2012, so negotiations on a new agreement began[216] .

In the meanwhile, the Treaty of Lisbon that had entered into force gave the Parliament the power to influence final decisions on international agreements. Considering the criticism that the Parliament had previously raised on privacy issues, many would have expected the European institution to put a veto on the new draft concluded by the Council in 2011. When the draft passed through the Parliament in 2012, after a positive opinion of the LIBE, surprisingly, it was approved. This time, political and diplomatic concerns prevailed over concerns regarding the protection of fundamental rights[217], but it has to be noticed that privacy protections had been improved by the new draft, and that a large minority of the European

[213] Joint Statement of the EC and CBP, Bruxelles, February, 2003.

[214] "European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights", European Parliament Resolution P5_TA(2003)0097, March 13, 2003. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P5-TA-2003-0097+0+DOC+XML+V0//EN.

[215] (C-317/04); (C-318/04).

[216] Arianna Vedaschi, and Gabriele Marino Noberasco, "From DRD to PNR: Looking for a New Balance Between Privcay and Security", in *Surveillance, Privacy and Trans-Atlantic Relations*, eds. David Cole, Federico Fabbrini, Stephen Schulhofer (Hart Publishing: 2017).

[217] Sylvie Peyrou, "Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne", *Revue Europe*, No. 7 (Juillet 2012).

Parliament's members voted against the draft[218]. The general internal disagreement of the EU Parliament and the pressure received by the Council for the finalization of a PNR agreement made the discussion about privacy and security continue within the Parliament.

Negotiations between the EU and the USA about flows of PNR data started at the end of 2003 and were concluded only in 2012. It took 9 years before the two parties reached a final decision. At this point, it is important to highlight some differences between the EU and the USA.

On the European side, negotiations with the United States started only after the decision of the US to systematically collect the entire massive amount of information on all the passengers flying to the US following the 9/11 terrorist attacks, because of major concerns that started to be raised within the European Union regarding the respect of the EU Data Protection Directive.[219] However, some several control mechanisms that were put in place were quite fundamental for ensuring the protection of EU citizens' privacy. Indeed, the Parliament stepped in the negotiation process with the US numerous times requiring more safeguards for the protection of privacy. Moreover, during the 9 years of negotiations, when consensus seemed to be reached on the European side, either the European Court of Justice or the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament intervened to invalidate the agreement and to reject the amended draft agreement on privacy protection grounds, respectively.

While the European Union struggled to reach a final decision, the United States has always pushed for the finalization of the agreement. However, the reader should keep in mind that, as previously noticed in this chapter, the protection of privacy in the United States is extremely different than in Europe. As explained, the 1974 Privacy Act did not apply to EU citizens until 2015. The fact that the Act discriminated in protecting people has raised many concerns, notably when the US government initiated negotiations with the EU for the PNR Agreement.

Understanding the reasons behind the pressure put on the Parliament for the approval of the EU-US PNR Agreement is fundamental to clarify that privacy and security played a significant role during the negotiations. As for the role of security, it is very enlightening to notice that the first version, namely the version with the lowest level of privacy guarantees, has been approved after an increase in the perception of security threat in the EU. Indeed, it was approved by the Council right after the 2004 Madrid terrorist attacks, which caused an increase in the perception of threat[220].

---

[218] "Parliament gives green light to air passenger data deal with the US", *European Parliament Press Release*, April 19, 2012. Available at: http://www.europarl.europa.eu/news/en/news-room/20120419IPR43404/parliament-gives-green-light-to-air-passenger-data-deal-with-the-us.

[219] Hiroyuki Tanaka, Rocco Bellanova, Susan Ginsburg and Paul De Hert, *Transatlantic Information Sharing: At a Crossroads* (Washington, DC: Migration Policy Institute, 2010), p.16.

[220] Javier Argomaniz, The EU and Counter-Terrorism: Politics, Polity and Policies After 9/11 (Routledge, 2010), pp. 129-130.

It should also be noticed that, although in the end the EU reached a decision, there has always been much disagreement on the PNR case within the Union. On the one hand, the agreement is considered as being extremely important because it is crucial for the intelligence to have information on the movement of people, especially considering the recent phenomenon of the foreign fighters. On the other hand, skepticism on the effectiveness of the PNR Agreement and critiques concerning privacy have been significant. For instance, in January 2015, in an intervention at the LIBE Commission, the European Data Protection Supervisor Giovanni Buttarelli heavily criticized the PNR system. In his speech, he admitted his skepticism towards the indiscriminate storage of data of the PNR, since he could not see how such a system could be useful to prevent terrorist attacks such as the Charlie Hebdo tragedy[221].

[221] "La società sorvegliata", *Garante Privacy,* Atti del Convegno, January 8, 2016, p. 69. Available at: http://194.242.234.211/documents/10160/5312012/La+societ%C3%A0+sorvegliata+-+Atti+del+convegno+del+29+gennaio+2016.

CONCLUSION

Insights from EU-USA cooperation on information-sharing

This dissertation showed that since the current literature on information sharing focuses on security issues as the main barrier to cross-border information sharing, it fails to take into account the real factors that may constitute a serious impediment to this process. The approval of the first version of the EU-US PNR agreement after terrorist attacks exemplifies the importance of considering the level of perception of security threat as the main boost for sharing information, thus being proof of the failure of the literature analyzed in the first chapter to recognize security as a cause of rather than a barrier to cross-border information exchange. Studies on the processes of international negotiations recognize that domestic interests play an important role, but no academic research investigates the role of domestic factors in international negotiation processes on the exchange of information.

This thesis has focused in particular on the study of the response of the United States and the European Union to the intensification of terrorist attacks and their cooperation on information sharing, analyzing the roles of security and privacy in the process of negotiations. It is clear that the EU and the USA do not guarantee the same level of protection of privacy. While the higher level of privacy of the European Union does not constitute a threat to the value of security, it caused many difficulties during the negotiations with the United States on the exchange of information. By contrast, a poor protection of privacy allows the US to focus more on security issues and push for negotiations for sharing information.

This dissertation has demonstrated the importance of security and privacy in the context of information sharing. Even if security is a value which might be regarded in different ways with respect to other values, its importance is undeniable and is recognized by the international community, including the United States and the European Union. The development of IT and the new means that this development provided to the intelligence agencies of the two international actors have encouraged them to share more information. This has been concretely demonstrated throughout the dissertation, and in particular in the section about the EU-USA PNR agreement. Indeed, an increase in the perception of terrorist threat caused a positive development for the negotiations. While security represents a boost for the progress of negotiations both at domestic (regional in the case of the European Union) and at EU-US level, the protection by the European Union of its legal environment represented a serious obstacle for the finalization of the PNR agreement. Thus, a difference in the level of privacy can be considered as a barrier to the process of

agreement-making on information sharing between the EU and the USA. Indeed, steps towards the harmonization of privacy guarantees have enhanced their cooperation.

How to deepen EU-USA cooperation on information-sharing

Since the problem of the EU-US cooperation on information sharing for security purposes is the different level of privacy, and in the light of the recent step towards the EU concerns on privacy by the US through the Redress Bill, one could wonder if harmonizing privacy protection could be a possible solution. However, absolute harmonization of legislation is unluckily. This is due to different reasons that have been anticipated in the previous chapters. First of all, the cultural strategy of the USA makes politicians more prone to adopt questionable measures and justify them on grounds of national security. Secondly, EU and USA people attribute a different importance to the values of security and privacy. These reasons also make the idea of establishing international institutions or agencies for the exchange of information extremely complicated. However, the creation of "international and regional centers to exchange data on methods of defense and response"[222] of the policymakers, intelligences and legislative authorities could be useful to enhance counterterrorism cooperation. Thus, sharing information on different legal responses (in terms of law or regulatory enforcements, legal solutions) or intelligence training could be an option. Improving transparency would also be an optimal solution, because it would increase the level of trust in law enforcement authorities. It is important to stress the fact that at the heart of representative democracies stays transparency and accountability. The whole discourse about balancing privacy and security would not make sense for countries that are not representative democracies. An excessive level of secrecy, indeed, is a friend of terrorism. As Tuomas Ojanen, Cian Murphy and Federico Fabbrini notice, the use of secrecy in measures that are resorted to combat terrorism may have a negative impact on rights[223]. They demonstrate that since some international decisions are takes on the basis of classified information, even when disclosure of evidence is demanded by a party in order to defend its rights against that decision, there is no possibility to have access to information that has been classified by a state. Thus, cross-border information sharing is certainly a huge step towards a counterterrorism regime based on a more effective protection of rights. Constitutional law has greatly improved in addressing problems that are due to the excessive use of secrecy by executive powers. Indeed, the increasing interaction between legislative and judicial branches, and between national and supranational regimes ensures a more effective observance of constitutional values.

[222] Anthony H. Cordesman, and Alreigh A. Burke, "International Cooperation in Counterterrorism: Redefining the Threat and the Requirement", *Center for Strategic and International Studies*, March 11, 2010.
[223] David Cole, Federico Fabbrini and Arianna Vedaschi, "Secrecy, National Security and the Vindication of Constitutional Law" (Edward Elgar, 2013), p. 7-8.

Differently from the case of the USA, the European Union members are more prone to contrast the abuse of secrecy by their governments justifies by reasons of national security. An example is the case of Germany, where the Constitutional Court "reinforced the right of the German Parliament to obtain classified information from the executive and at the same time annulled legislation which unduly restricted privacy rights in the interests of surveillance and public safety"[224]. Instead, the American "executive branch demands for deference generally inhibit the willingness of the judiciary to use their existing capacities effectively to oversee executive recourse to secrecy"[225]. If on the one hand, the need for secrecy for counterterrorism operations is not doubted, on the other hand, the legitimacy of secrecy cannot allow "deviations from principles of the rule of law, transparency and accountability"[226], and an active judiciary in balancing security need with public interest values is crucial for this purpose.

As for the United States, it is clear that it lacks proper supervision over the activities of the intelligence[227]. Thus, independent oversight bodies and some control mechanisms should be established in order to firstly, guarantee the protection of the privacy of US citizens, and secondly, increase its credibility as an international actor in the protection of fundamental rights and international treaties. A stronger protection of privacy, in turn, would favor "a stronger confidence between law enforcement authorities and strengthen(…) legal certainty"[228].

More generally speaking, having provided the reader with some basic knowledge on information sharing, this thesis encourages further research in this area in order to better fill the current gap in the literature on the roles of security and privacy and their influence on processes of data exchange.

Bibliography

[224] Mindia Vashakmadze, "Secrecy vs. openness: counterterrorism and the role of the German Federal Constitutional Court", in *Secrecy, National Security and the Vindication of Constitutional Law*, eds. David Cole, Federico Fabbrini and Arianna Vedaschi (Edward Elgar, 2013).

[225] Stephen Schulhofer, "Oversight of national security secrecy in the United States", *Secrecy, National Security and the Vindication of Constitutional Law*, eds. David Cole, Federico Fabbrini and Arianna Vedaschi (Edward Elgar, 2013), pp. 22-43.

[226] D. Cole et al., p. ix.

[227] Robyn R. Mace, "Intelligence, Dataveillance, and Information Privacy", *Protecting Persons While Protecting the People*, eds.Cecilia S. Gal, Paul B. Kantor, and Michael E. Lesk, (Springer, 2009), p. 42.

[228] "Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalized World", *European Commission*, January 10, 2017, p.13.

ONLINE SOURCES:

"Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program", Preamble. Text available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2010.195.01.0003.01.ENG&toc=OJ:L:2010:195:TOC#L_2010195EN.01000501.

"Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalized World", European Commission, January 10, 2017. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN.

"Critically assess the similarities and differences in foreign policy between the administrations of George W. Bush and Barack Obama", *Clumpjack*, January 16, 2015. Available at: https://clumpjack.wordpress.com/2015/01/16/critically-assess-the-similarities-and-differences-in-foreign-policy-between-the-administrations-of-george-w-bush-and-barak-obama/.

"Europeans' attitudes towards security", *Special Eurobarometer 432* (April, 2015). Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_432_sum_en.pdf.

"Follow-up to Concluding Observations", *Center for Civil and Political Rights.* Available at: http://ccprcentre.org/page/114th-session-in-brief/follow-up-to-concluding-observations?/114-session-follow-up-concluding-observation/.

"General Assembly Adopts Resolution Affirming Importance of Balanced, Integrated Implementation of Global Counter-Terrorism Strategy", *UN Press*, GA/11800, July 1, 2016. Available at: https://www.un.org/press/en/2016/ga11800.doc.htm.

"Information society, privacy and data protection", *European Union Agency for Fundamental Rights.* Available at: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection.

"La società sorvegliata", *Garante Privacy*, Atti del Convegno, January 8, 2016, p. 167. Available at: http://194.242.234.211/documents/10160/5312012/La+societ%C3%A0+sorvegliata+-+Atti+del+convegno+del+29+gennaio+2016.

"Lotta dell'UE al terrorismo", *Consilium*. Available at: http://www.consilium.europa.eu/it/policies/fight-against-terrorism/.

"May 25, 2017: Secretary General Stoltenberg's Doorstep at the NNHQ", U.S. Mission to the North Atlantic Organization, May 25, 2017. Available at: https://nato.usmission.gov/may-25-2017-secretary-general-stoltenbergs-doorstep-nnhq/.

"National Strategy for Information Sharing: Successes and Challenges In Improving Terrorism-Related Information Sharing" *Nationwide Sar Initiative,* October 2007. Available at: https://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf .

"NATO and the fight against terrorism", Transcript of Ambassador Sorin Ducaru, November 6, 2014. Available at: http://www.nato.int/cps/en/natohq/opinions_114693.htm.

"Parliament gives green light to air passenger data deal with the US", European Parliament Press Release, April 19, 2012. Available at: http://www.europarl.europa.eu/news/en/news-room/20120419IPR43404/parliament-gives-green-light-to-air-passenger-data-deal-with-the-us.

"Privacy and data protection by country", *Forrester Research.* Available at: http://heatmap.forrestertools.com/.

"Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes — SWIFT", 2007/C 166/09 . Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1416847896590&uri=CELEX:22007X0720(02).

"Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime", Opinion 5/2015 EDPS, September 24, 2015. Available at https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf.

"The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid", *Court of Justice of the European Union Press Release*, No. 117/15, Luxembourg, October 6, 2015. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

"The Stockholm Programme", *Eur-Lex*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Ajl0034.

"U.S. Receives Low Grades on Privacy and Surveillance from UN Committee", *Brennan Center for Justice,* July 18, 2015. Available at: https://www.brennancenter.org/press-release/us-receives-low-grades-privacy-and-surveillance-un-committee.

"What is Privacy?", *Privacy International.* Available at: https://www.privacyinternational.org/node/54.

"Yates, Clapper To Testify In Senate Hearing On Russian Election Meddling" , NPR, April 25, 2017. Available at: http://www.npr.org/sections/thetwo-way/2017/04/25/525542524/yates-clapper-to-testify-in-open-house-hearing-on-russian-election-meddling.

Boehm, Franziska; and Cole, Mark D., "Data Retention after the Judgment of the Court of Justice of the European Union" (June 30, 2014), p. 48. Available at: https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf.

Buffet, Francois-Noel (au nom de la commission d'enquête), "Circuler en sécurité en Europe: renforcer Schengen", Rapport No. 484 (2016-2017), March 29, 2017.

Cavoukian, Ann; and Jonas, Jeff, "Privacy by Design in the Age of Big Data", June 8, 2012, p. 7. Available at: https://datatilsynet.no/globalassets/global/seminar_foredrag/innebygdpersonvern/privacy-by-design-and-big-data_ibmvedlegg1.pdf.

Clarke, Sarah, "The Dissident Blog's Issue #17 – Digital Threats", *Pen International*, July 8, 2015. Available at: http://www.pen-international.org/07/2015/mass-surveillance-and-online-censorship-the-pen-international-prespective/.

Curry, Tom, "Obama continues, extends some Bush terrorism policies", *NBC News*, June 6, 2013. Available at: http://nbcpolitics.nbcnews.com/_news/2013/06/06/18804146-obama-continues-extends-some-bush-terrorism-policies?lite.

Hsu, Richard, "Government Surveillance Under a Trump Administration", *Shearman and Sterling*, December 19, 2016. Available at: http://www.shearman.com/en/newsinsights/publications/2016/12/govr-surveillance-under-a-trump-administration.

Josh Meyer; and Greg Miller, "Secret U.S. Program Tracks Global Bank Transfers", *Los Angeles Times*, June 23, 2006. Available at: http://articles.latimes.com/2006/jun/23/nation/na-swift23.

Jourová, Věra "The future of U.S.-EU data transfer arrangements at the Brookings Institution" *European Commission Press Release Database* (Speech/156104). Available at: http://europa.eu/rapid/press-release_SPEECH-15-6104_en.htm.

Kelly, Sanja; Earp, Madeline; Reed, Laura; Shahbaz, Adrian; and Truong, Mai, "Tightening the Net: Governments Expand Online Controls, Freedom on the Net (2014)", *Freedom House.* Available at: https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf.

Kirkhope, Timothy, "Eu-Passenger Name Record (European PNR)", *Europarl* (2016). Available at: http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-eu-passenger-name-record-(european-pnr).

Lichtblau, Eric; and Risen, James, "Bank Data Is Sifted by U.S. in Secret to Block Terror", *New York Times*, June 23, 2006. Available at: http://www.nytimes.com/2006/06/23/washington/23intel.html;

Miglietti, Lucia, "Profili storico-comparativi del diritto alla privacy", *Diritti Comparati*, December 4, 2014. Available at: http://www.diritticomparati.it/2014/12/profili-storico-comparativi-del-diritto-alla-privacy.html.

Nojeim, Greg, "When Metadata Becomes Megadata: What the Government Can Learn", *CDT*, June 17, 2013. Available at: https://cdt.org/blog/when-metadata-becomes-megadata-what-the-government-can-learn/.

Opinion 10/2006 (WP128) on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), November 22, 2006, p.14. Available at: http://www.dataprotection.ro/servlet/ViewDocument?id=234.

Parlapiano, Alicia, "Comparing Two Secret Surveillance Programs", *The New York Times*, June 7, 2013. Available at: http://www.nytimes.com/interactive/2013/06/07/us/comparing-two-secret-surveillance-programs.html?_r=0.

Press Release on the SWIFT Case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), November 23, 2006. Available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2006/pr_swift_affair_23_11_06_en.pdf.

Romano, Luca, "Nizza, Berlino, Londra, Stoccolma. Gli attacchi terroristici con camion e auto", *il Giornale.it.* Available at: http://www.ilgiornale.it/news/mondo/nizza-berlino-londra-stoccolma-attacchi-terroristici-camion-1383630.html.

Sainato, Michael, "Former NSA Senior Analyst Blasts Obama and Bush for Enabling Deep State Crisis", *Observer*, September 3, 2017. Available at: http://observer.com/2017/03/nsa-senior-analyst-deep-state-crisis/.

Simpson , Glenn R., "U.S. Treasury Tracks Financial Data In Secret Program", *Wall Street Journal*, June 23, 2006. Available at: https://www.wsj.com/articles/SB115101988281688182.

Snider, Mike and Weise, Elizabeth, "EU, U.S. agree on data sharing pact", *USA Today*, July 12 2016. Available at: http://www.usatoday.com/story/tech/news/2016/07/12/eu-us-agree-privacy-shield-data-rules/86980774/.

TNS public & social, "Public opinion in the European Union", *Standard Eurobarometer 83*, July, 2015. Available at: http://ec.europa.eu/public_opinion/archives/eb/eb83/eb83_first_en.pdf.

U.S. House of Representatives, "The Terror Finance Tracking Program: hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services", 109th Congress, Second Session, July 11, 2006 (Washington: U.S. G.P.O., 2007).

ARTICLES:

Archick, Kristin, "U.S.-EU Cooperation Against Terrorism", *Congressional Research Service* (July 9, 2010).

Baldwin, David A., "The concept of security", *Review of International Studies,* No.23 (1997), pp. 5-26. Available at: http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf.

Best, Richard A. Jr., "Sharing Law Enforcement and Intelligence Information: The Congressional Role", *Congressional Research Service*, February 13, 2007. Available at: https://fas.org/sgp/crs/intel/RL33873.pdf.

Bigo, Didier; Carrera, Sergio; Guild, Elspeth; and Mitsilegas Valsamis, "The EU and the 2016 Terrorist Attacks in Brussels: Better instead of more information sharing", *CEPS Commentary*, April 6, 2016. Available at: https://www.ceps.eu/publications/eu-and-2016-brussels-terrorist-attacks-better-instead-more-information-sharing.

Caprioli, Eric A., "Violation des règles propres aux données à caractère personnel et réseau SWIFT", *Revue de Droit bancaire et financier,* No. 1 (January 2007).

Casale, Davide, "EU Institutional and Legal Counter-terrorism Framework", *Defence Against Terrorism Review*, Vol. I, No.1 (2008), pp.49-77.

Conces, Rory J., "Rethinking Realism (or Whatever) and the War on Terrorism in a Place like the Balkans", *Theoria: A Journal of Social and Political Theory,* No.120 (2009), pp. 81-124. Available at: http://www.kakanien-revisited.at/beitr/theorie/RConces3.pdf.

Cordesman, Anthony H., and Burke, Alreigh A., "International Cooperation in Counterterrorism: Redefining the Threat and the Requirement", *Center for Strategic and International Studies*, March 11, 2010.

Damon, Lisa J., "Freedom of Information versus National Sovereignty: The Need for a New Global Forum for the Resolution of Transborder Data Flow Problems", *Fordham International Law Journal*, Vol. X, Issue 2 (1986), pp. 260-287.

De Burca, Grainne, "The European Court of Justice and the International Legal Order After Kadi", *Harvard International Law Journal*, Vol. LI, No. 1, (2010).

De Goede, Marieke, "The SWIFT Affair and the Global Politics of European Security", JCMS, Vol. L, Issue 2 (March, 2012), pp. 214–230.

De Vasconcelos, Álvaro; and Zaborowski, Marcin, "The Obama Moment: European and American Perspectives", *EU Institute for Security Studies*, (2009). Available at: http://www.iss.europa.eu/uploads/media/The_Obama_Moment__web_A4.pdf.

Den, Monica, "9/11 and the Europeanisation of Anti-Terrorism Policy: a Critical Assessment", Groupement D'études et de recherchés, *Policy Paper,s* No.6, (2003). Available at: http://ftp.infoeuropa.eurocid.pt/files/database/000005001-000010000/000007639.pdf.

Donald, Alice; Gordon, Jane; and Leach, Philip, "The UK and the European Court of Human Rights", *Equality and Human Rights Commission*, No. 83 (2012).

Eriksson, Johan; and Giacomello, Giampiero, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", *International Political Science Review,* Vol. XXVII, No. 3 (July, 2006), pp. 221-244.

Hoeft, Gabriel, "'Soft' Approaches to Counter-Terrorism: An Exploration of the Benefits of Deradicalization Programs", *International Institute for Counter-Terrorism* (2015). Available at: https://www.ict.org.il/UserFiles/ICT-Soft-Approaches-to-CT-Hoeft.pdf.

Hoffman, Bruce, "Is Europe Soft on Terrorism?", *Foreign Policy*, No.115 (1999), pp. 62-76.

Hong, Kwo-Shing; Chi, Yen-Ping; Chao, Louis R.; and Tang, Jih-Hsing, "An integrated system of information security management"*, Information Management & Computer Security,* Vol. XI, Issue 5 (2003) pp. 243-248. Available at: http://kczx.shupl.edu.cn/download/85fbe28e-f3a4-4765-a41a-95f5b71d2c31.pdf.

Huie, Marsha Cope; Laribee, Stephen F.; and Hogan, Stephen D., The right to privacy in personal data: the EU prods the US and controversy continues, *Tulsa Journal of Comparative and International Law*, Vol. IX, Issue 2 (2002), pp. 391-469.

Jackson, Richard, "Culture, identity and hegemony: Continuity and (the lack of) change in US counterterrorism policy from Bush to Obama", *International Politics,* Vol. XLVII (March, 2011), pp. 390-411.

Jonas, Jeff; and Harper, Jim, "Effective Counterterrorism and Limited Role of Predictive Data Mining", *Policy Analysis*, No. 584 (December 11, 2006). Available at: https://object.cato.org/pubs/pas/pa584.pdf.

Keohane, Daniel, "The EU and counter-terrorism", *CER* (May, 2005).

Kierkegaard, Sylvia, "US War on terror EU swift(ly) signs blank cheque on EU data", *Computer Law & Security Law Review,* No.27 (2011), pp. 451-464.

Kühling, Jürgen; and Heitzer, Sonja, "Returning through the national back door? The future of data retention after the ECJ judgment on Directive 2006/24 in the UK and elsewhere", *European Law Review*, April, 2015, pp.263-278. Available at: https://ael.eui.eu/wp-content/uploads/sites/28/2015/04/Spaventa-08-Kuhling-Heitzer.pdf.

Leavitt, Harold J., and Whisler, Thomas L., "Management in the 1980's", *Harvard Business Review*, November, 1958. Available at: https://hbr.org/1958/11/management-in-the-1980s.

Morgan, Mathew J., "The Origins of the New Terrorism", *Parameters,* Vol. XXXIV, No.1 (2004), pp. 30-31.

Peyrou, Sylvie, "Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne", *Revue Europe,* No. 7, July, 2012.

Putnam, Robert D., "Diplomacy and Domestic Politics: The Logics of Two-Level Games", *International Organization,* Vol. XLII, No. 3 (1988), pp. 427-460.

Rees Wyn; and Aldrich, Richard J., "Contending cultures of counterterrorism: transatlantic convergence or divergence?", *International Affairs*, Vol. LXXXI, Issue 5 (October, 2005), pp. 905-923.

Robert O. Keohane, "International Institutions: Can Interdependence Work?", *Foreign Policy,* No. 110 (Spring, 1998).

Romaniello, Maria, "The international role of the European Parliament: the SWIFT Affair and the 're-assessed' European institution balance of power", *Perspectives on Federalism,* Vol. V, Issue 1 (2013).

Santolli, Justin, "The Terrorist Finance Tracking Program: Illuminating the shortcomings of the European Union's antiquated data protection directive", *The George Washington International Law Review,* Vol. XL, No. 2 (2008), pp.553-582. Available at: http://docs.law.gwu.edu/stdg/gwilr/PDFs/40-2/40-2-6-Santolli.pdf.

Schütze, Robert, "From Dual to Cooperative Federalism: The Changing Structure of European Law", *European Journal of International Law*, Vol. XXI, Issue 4 (Oxford University Press, 2010).

Sjoberg, Lennart, "Political decisions and public risk perception", *Reliability Engineering & System Safety*, Vol. LXXII, Issue 2 (May, 2001), pp. 115-123.

Slovic, Paul, "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield", *Risk Analysis*, Vol. XIX, Issue 4, (August, 1999) pp. 689-701.

Swire, Peter P. "Privacy and Information Sharing in the War on Terrorism", *Villanova Law Review,* Vol. LI (2006), pp.101-129.

Tridimas, P. Takis, "EU Law, International Law and Economic Sanctions Against Terrorism: The Judiciary in Distress?", 32 *Fordham Int'l L.J.,* 660 (2009).

Tzanou, Maria, "The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance", *Modern Studies in European Law,* No. 71 (Hart Publishing, June 1, 2017).

Zuccotti, Susan, "The Italian Racial Laws, 1938-1943: A Reevaluation", in "The Fate of the European Jews, 1939-1945: Continuity or Contingency?", (ed.) Jonathan Frankel, *Studies in Contemporary Jewry*, Vol. XIII (Oxford University Press: 1998).

BOOKS:

Adler, Emanuel; and Barnett, Michael, *Security Communities* (Cambridge University Press , 1998).

Argomaniz, Javier, *The EU and Counter-Terrorism: Politics, Polity and Policies After 9/11* (Routledge, 2010).

Aspray, William; and Doty,Philip Doty (eds.), *Privacy in America* (Lanham, UK: The Scarecrow Press, Incs, 2011).

Camilleri, Joseph A.; and Falk, Jim, *The End of Sovereignty? The Politics of a Shrinking and Fragmenting World* (Aldershot, UK: Edward Elgar, 1992).

Cole, David; Fabbrini, Federico; and Schulhofer, Stephen (eds), *Surveillance, Privacy and Trans-Atlantic Relations* (Hart Publishing: 2017).

Cole, David; Fabbrini, Federico; and Vedaschi, Arianna, *Secrecy, National Security and the Vindication of Constitutional Law* (Edward Elgar, 2013).

Collier, Ruth Berins; and Collier, David, *Shaping the political arena: critical junctures, the labor movement and regime dynamics in Latin America* (Princeton: Princeton University Press, 1991).

De Burca, Grainne; Halevi, Joseph; and Weiler, Horowitz, *The Worlds of European Constitutionalism* (Cambridge University Press, 2011).

Fabbrini, Sergio, *Democracy and Federalism in the European Union and the United States* (Routledge, 2005).

Ferreira-Perreira, Laura C. and Martins, Bruno Oliveira, *The European Union's Fight Against Terrorism: The CFSP and Beyond* (Routledge, 2014).

Gal, Cecilia S.; Kantor, Paul B.; and Lesk, Michael E. (Eds.), *Protecting Persons While Protecting the People* (Springer, 2009).

Ganor, Boaz, *The Counter-Terrorism Puzzle: A Guide for Decision Makers*, (2005).

Jarvis, Lee; MacDonald, Stuart; and Chen, Thomas M., *Terrorism Online: Politics, Law and Technology* (Routledge, 2015).

Lennon, Genevieve; and Walker, Clive (eds), *Routledge Handbook of Law and Terrorism* (Abingdon, OX: Routledge, 2015).

Netanyahu, Benjamin, *Terrorism - How the West Can Win* (Avon Books,1986).

Nye, Joseph S. Jr., *Soft Power, The Means to Success in World Politics* (New York: Public Affairs, 2004).

Ramraj, Victor V.; Hor, Michael; and Roach, Kent, *Global Anti-Terrorism Law and Policy* (Cambridge University Press, 2005).

Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Caroline Press: 2009).

Renshon, Stanley A., *National Security in the Obama Administration: Reassessing the Bush Doctrine* (Routledge, 2010).

Siegel, Larry J., *Criminology: Theories, Patterns, and Typologies*, 12th ed. (Cengage Learning, 2015).

Solove, Daniel J, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press, 2011).

Tanaka, Hiroyuki, Bellanova, Rocco, Ginsburg, Susan and Hert, Paul De, *Transatlantic Information Sharing: At a Crossroads* (Washington, DC: Migration Policy Institute, 2010).

Waltz, Kenneth, *Theory of International Politics* (Addison-Wesley, 1987).

SUMMARY

The terrorist attack of 9/11, followed by the escalation of the terrorist menace in the West, proved the inefficiency of intelligence agencies. From that moment on, in the light of the exponential improvement in the field of Information Technology (IT), sharing sensitive information became central to the fight against terrorism. This dissertation analyzes the cooperation on information sharing between the United States and the European Union as a response to the terrorist threat after the events of 9/11. The main objective is to understand the role of the values of security and privacy in the development of the bilateral negotiations on the exchange of data, trying to answer the question: how do privacy and security influence the EU-US cooperation on information sharing against terrorism? Moreover, this above question is meaningful for the enrichment of the literature on information sharing and the debate on the contrasting values of privacy and security, and will contribute to help international actors to understand the steps they should take to improve cooperation in the field of information sharing.

As for the role of security, most of the literature doesn't recognize it as a factor that may actually boost the exchange of information, consequently failing in indentifying real barriers to information sharing. Most of the literature that has manifested the interest in studying the role of information focused on states' concern over a possible erosion of national sovereignty and issues of domestic instability. This topics gained attention because globalization and, with it, economic integration and technological development contributed to redefining the concept of national sovereignty. This first part of the literature noticed that, even though globalization inhibits states from fully controlling information flows due to the absence of a global regulator of the Internet, states continue to retain massive amounts of information for security reasons. Academic studies provide different concepts of security. Realists look mainly at national security, and those studies who expand the notion of national security tend to include mainly its economic dimension, especially for IT-related security threats (e.g. cyber-threats that can disrupt the economy and political order of a state). Even liberals, who have always included other dimensions of security – be them economic, environmental, human – have identified in economic aspects the costs of inter-state connection. Thus, most researches explain that states retain and want to control flows of information for security reasons, focusing on concepts of national security or on the economic dimension of security.

Nye points out that shared values explain cooperation. A second part of the literature does consider security as a shared value and believes in the existence of security communities, in which cooperation ensures peace. Indeed, the logic behind the idea of a world dominated by anarchy and the predominance of national security interests over international interests and shared values is inconsistent with reality. Reality shows that security is one of the main values that are shared within the international community (see, for example, Art.1 of the Charter of the UN; Preamble and Art. 3 of TEU; Art.1 NATO; Preamble and Art. 6 Charter of Fundamental Rights of the EU; Preamble and Art. 5 European Convention on Human Rights). Thus, being the interest of maintaining security a shared value, it explains the willingness of states to cooperate. This second logic

suggests that security might be a reason to engage in negotiations on information sharing. Indeed, one way in which states cooperate on security is through the "need to share" approach, which has increasingly become a critical part of states' policies after the emergence of asymmetric threats.

However, evidence shows also that processes of international cooperation on information sharing are slow, and it is difficult to reach consensus on a final agreement during negotiations. If, on the one hand, the fact that two actors share values and want to promote similar interests can explain the willingness to cooperate, on the other hand, it's not implied that the process that leads to cooperation will be unimpeded and unchallenging. In order to detect the factors that impede international actors from reaching agreements on information sharing, a more in-depth study of negotiation processes is necessary, since the existing literature not only lacks exhaustive studies on information sharing in general, but also falls short of theoretical results on negotiation processes for the exchange of information. Thus, in cases in which the maintenance of security is an explanation for cooperation on information sharing, what can explain the lethargy of negotiations?

This thesis argues that privacy is a barrier to information sharing. The literature does recognize that the new information era provokes privacy concerns. However, scholars are divided on defining the relation between privacy and security. Part of the literature considers privacy and security as opposing and conflicting values. On the contrary, other academics insist on the fact that those views that oppose privacy and security are misleading, and talk about a "false trade-off" between these two values.

The theoretical framework of this dissertation is based on two assumptions. The first assumption, which derives from the two-level game theory, is that the weight of different domestic interests matters when it comes to the study of international agreement-making processes. The second assumption is that the international aim and national interest to maintain security facilitates the initiation of negotiations on information sharing. Thus, an increase in the level of perception of security threats speeds up the process of negotiation. The hypothesis is grounded especially on the first assumption of this thesis, namely that the domestic level is essential for studying negotiation processes on agreements on information sharing. Hence, it is reasonable to believe that there is something at regional level in the European Union and at domestic level in the United States that blocks the bilateral process of negotiations on information sharing. The hypothesis is that the protection of privacy is a barrier to international cooperation on information sharing, thus, two cases characterized by different privacy protection levels should be studied. In order to test the hypothesis, this dissertation will consider the European Union and the United States, which are characterized by a higher and lower level of privacy, respectively. Understanding the concepts of security and privacy and contextualizing them in the fight against terrorism in the EU and the USA is necessary to show how the value that the two international actors attribute to security and privacy influences their cooperation on information sharing. While security is a reason to engage in this kind of cooperation, the differences in the

legal frameworks concerning privacy prove to be great obstacles to the finalization of agreements that regulate the exchange of data.

The second chapter of this thesis begins by exploring the role of security at the international level, and the development of security communities, especially following the emergence of the threat of terrorism. It considers the importance of the need of sharing information, as well as the emergence of obstacles in the cooperation on information sharing.

The international political discourse concerning problems of security has been dominated by the realist tradition and its variations. According to realism and neorealism, the international politics is characterized by the struggle for power and the prevalence of an anarchic international system in which the principal actor is the nation-state. According to Waltz, the main value that influences states' policies is national security. The traditional realist idea of security focuses on the role of the state and it is strictly related to military security. After the Cold War, the survival of the traditional concept of security was undermined by various changes, among which the menace of Islamic terrorism. Firstly, the terrorist attacks of 2001 and the subsequent emergence of a transnational problem that involves actors at all levels (NGOs, International Organizations, States, etc) weakened the traditional vision of security linked to national territory. Secondly, the enemies that began to perpetuate the attacks were non-state actors, which replaced the traditional subjects that had been involved in wars until that moment, namely state actors. Thus, the so-called "War on Terrorism" cannot be associated with the traditional idea of war: the boundaries of states do not matter anymore and the traditional means of deterrence are not effective. Many authors refer to a "new terrorism" or "post-modern terrorism", also because of the non-traditional means used to perpetuate an attack (biological, nuclear, etc).

As a consequence of the changing international environment and the emergence of new threats, the entire discourse about anarchy and the prevalence of national interests which dictate national foreign policies became vane. Security proved to be "a main motive for integration". Right after the two World Wars, history assisted to an era of institution building (NATO, UN, OSCE, etc) and to the emergence of the so-called "security communities" that shared a common objective: the maintenance of peace and security. In the context of the rising terrorist threat and the new characterizations of terrorism, the already existing international organizational framework for cooperation on security rapidly turned its attention, resources and efforts to repress Islamist ideologies and fundamentalism. One way in which the security communities began to cooperate was through the share of information and intelligence, but not without difficulties. Indeed, international cooperation on information sharing is influenced by the secrecy that intelligence forces attribute to the information they collect, which creates barriers between intelligence and law enforcement agencies. Actually, the problem for this kind of cooperation is not the absence of legislation at international level on this subject: there are conventions and agreements at international level that regulate this

cooperation and encourage the share of more sensitive information (NATO's Intelligent Liaison Unit, the Global Coalition to Defeat ISIS, UN Resolution 2309 in which it supported the International Civil Aviation Organization (ICAO) calling the UN members to share more information related to terrorism, etc). As demonstrated by NATO, the European Union, OSCE, the UN, security communities do manifest the willingness to share information and cooperate in this sense. All around the world, projects for the creation of Information Sharing Environments (ISE) have been established in order to facilitate the exchange of information between national organizations and processes of cross-border sharing. However, in order to understand the difficulties that may obstacle this type of cooperation, it is important to first understand the reason why information is so valuable to security communities and what kind of information they are interested to share.

Intelligence agencies are interested in collecting and analyzing both Big Data and metadata, which serve the same scope. The analysis of data has an enormous potential in the field of security: through the analysis of all the information that a person leaves on the Internet, her profile can be reconstructed. In the light of the potential of data, democracies have laws that regulate their use and grant the protection of personal information, which is crucial for the survival of people's liberties. However, there is disagreement on the typology of data that have to be stored and processed in order to combat crimes. For example, the United States is more oriented towards an indiscriminate collection of data, while in the European Union the usefulness of a massive amount of personal data that are not collected with rationality is highly doubted. The disagreement between the EU and the USA on the methods used for risk-assessment purposes is mainly due to the increasing amount of concerns on the respect of fundamental rights that has emerged with the information age. Moreover, though the value of data mining in the fight against terrorism is widely recognized, the indiscriminate collection of data is criticized. Many researchers have great difficulties in identifying the potential of a counterterrorist strategy that relies on the analysis of massive amounts of data.

In order to understand what kinds of difficulties emerge in the context of information sharing within security communities, it is necessary to briefly introduce the general problem of respecting human rights while combating terrorism. The menace of terrorism has been used to legitimate state actions that erode the strength of fundamental rights. Generally speaking, fundamental rights are inalienable and cannot be violated. Thus, bypassing fundamental rights, as well as democratic values and fundamental liberties granted by the law at international level for security purposes is unacceptable, even if the case is to combat terrorism. This premise is necessary to understand the concerns that arise considering the increasing number of initiatives against terrorism that include sharing information, collecting and analyzing data and promoting mass surveillance programs for security purposes. The possibilities of application of IT have been used to profile people in the context of security. However, this process is negatively affecting civil liberties, leading to an authoritarian control of information and people. In the context of the fight against terrorism, the debate

about the contrast between security and human rights intensified, focusing in particular on the value of privacy, since it plays a decisive role in the era of information. Privacy is a right that is recognized in all modern societies. The right to privacy protects the properties and communications of people from external interference. It helps people defend themselves from abuses of power and grants them liberty. The right to protection of personal data can be derived from the general right to privacy. Especially after the emergence of asymmetric forms of terrorism and transnationalization of organized crime, the volume of data subject to surveillance policies has expanded, also thanks to technological improvements. Consequently, many other legislative instruments have been introduced to regulate the collection, storage, access and processing of personal data.

The questions that arise in the debate on privacy and security are the following: is the choice between security and privacy really a choice? On what grounds may a state possibly choose between privacy and security? What value prevails over the other? Those who support the idea of the primacy of security as a fundamental value use very powerful arguments to make people believe that giving up part of their privacy is necessary to achieve a safer environment. Opposing views to the arguments about the primacy of security try to demonstrate that the idea of choosing between the values of privacy and security is misleading. This category supports the "false tradeoff" theory, arguing that the idea of a tradeoff between the two values is based on false assumptions. Daniel J. Solove argues that coexistence of privacy and security is possible, it just needs oversight and regulation. The case of the European Union perfectly exemplifies the possibility of coexistence of privacy and security, which are both fundamental values and enjoy a very high level of protection. On the other hand, the idea of privacy and security as mutually exclusive values may be due to different reasons. Firstly, security necessities are much more understood by people with respect to privacy needs. Security has been defined as an inalienable public good, while privacy is underestimated and treated as a value belonging to the individual. This reasoning is particularly evident in the case of the United States, where the value of national security has always been preferred to the value of privacy.While privacy and security can coexist, it is very controversial to affirm that privacy and security are perfectly compatible values. Even in the case of the EU, where privacy is very much protected, contrasts between security and privacy issues frequently emerge.

In the third chapter it is much clearer that privacy issues in the United States are mostly due to lack of transparency and oversight of the government. This chapter is dedicated to the understanding of the role of security for these two actors taking into account their counterterrorism policies and cooperation. The Terrorist Finance Tracking Program (TFTP) case is used to provide a concrete example of the different value that the EU and the USA attribute to security.

After the terrorist attacks that the EU Member States and the United States have experienced, the European Union and the USA have become very active in the fight against terrorism. However, their cooperation in the

fight against terrorism has not always been easy, especially because of their extremely different responses to terrorism. While the United States adopted a hard approach, the European Union preferred a regulatory or legal approach. The literature on counterterrorism recognizes two different approaches, which are not necessarily mutually exclusive: the military approach and the legal approach. In the immediate aftermath of 9/11, while the United States adopted a "national security" and unilateral approach, the European Union relied on multilateralism.

The 9/11 events had a huge impact on the United States that led to the reaffirmation of the national security strategy, which reinforced the militaristic approach of the Bush Administration. The United States declared war on terrorism and began to invest a massive amount of resources on defense policies. As anticipated, the military and the legal approaches can coexist. Indeed, in the USA the national security structure rapidly changed and new agencies were created. However, the response of the United States was overall stronger than the EU response in terms of the prevalence of the use of force and national security justifications used to pass legislation which was subsequently criticized for disrespecting human rights. Indeed, the Congress soon expanded the powers of the intelligence and law enforcement authorities with the USA PATRIOT Act, and initiated activities of mass surveillance and secret programs of indiscriminate data collection and analysis. Moreover, the Bush Administration passed the Authorization for Use of Military Force (AUMF) in 2001, with which authorized the use of force against the perpetuators of the 9/11 attack. The USA also introduced the notion of "unlawful enemy combatant" through the Military Commission Act of 2006, which violated the Geneva Convention, that provides that all the persons not taking "active part in the hostilities" (for instance due to detention) should be treated humanely and respectfully. The national security urgencies of the United States, thus, led to the disregard of fundamental rights. The preference of the value of security by the USA surely affected the international image of the nation. In the eyes of the European Union, the American government's violations were inacceptable.

Differently from the United States, the response of the European Union mainly entailed a regulatory approach, which is supported and preferred at international level. The European regulatory response has also been referred to with other expressions as "legal" or "institutionalized", in the light of the establishment of an institutional system that is characterized by control mechanisms, strategies, conventions, and legal instruments for preventing terrorist attacks (e.g. Europol, Eurojust, European Public Prosecutor's Office) . For the European Union the respect the rule of law and fundamental rights is essential.

It is obvious that since the European Union and the United States have adopted different approaches in order to contrast terrorism, bilateral cooperation has not always been simple. However, after 9/11, EU-USA bilateral relationship improved for different reasons. A turning point, for instance, was the Obama Administration. Obama's agenda seemed to promote multilateralism in the governance of security, going beyond the traditional security framework of NATO. Consequently, the European Union started consider the

new aims of the USA as perfectly coinciding with its objectives in the security field. Even though Obama campaigned against many of Bush's domestic and foreign security operations, and proposed a different agenda, there have been some continuities with the precedent policies (use of force, military intervention, surveillance programs). Thus, the difficulty that characterizes the collaboration of the US and the EU on counterterrorism initiatives is still significant and the improvement of the relationship is very slow. This can be due to the fact that, as Rees and Aldrich affirm, while a shift in strategic doctrines is possible, a significant change in strategic cultures is rare. Strategic cultures are based on the past experience of a country, which is the key determinant of national threat perceptions and of the subsequent policies that are adopted in response to those perceptions. The realist ideology that has always been dominant in the USA had a significant impact on the policies of Obama's Administration, especially concerning issues related to security and the "War on Terror". However, the liberal ideology that enabled Obama to take some steps towards the promotion of multilateralism and the respect of the International Law, allowed a more successful dialogue with the EU and led to a gradual convergence of counterterrorist strategies.

The study of the Terrorist Finance Tracking Program (TFTP) is a pragmatic example of the hard-approach that was initially adopted by the United States after 9/11, and of the changing strategy towards multilateralism that characterized the Obama Administration, which enabled more cooperation with the European Union. In 2001, the USA Department of the Treasury initiated the TFTP, a secret program that obliged financial institutions operating in the USA to share all their information on financial transactions, which involved SWIFT, a Belgian company which collect most financial transactions, that had offices in Virginia. In June 2006, however, some American newspapers reported the existence of the TFTP and the monitoring activities of the government. This leak was particularly felt in the European Union, where the Data Protection Working Party established by Article 29 of the Directive 95/46/EC, the transfers violated different articles of the Directive, as well as the Belgian law. Due to the continuing concerns that were raised in the EU, SWIFT decided to stop operating in Virginia, thereby subtracting itself from the obligations of the TFTP. This forced the USA to initiate negotiations with the EU in order to access SWIFT data. The 2009 EU-US SWIFT Interim Agreement was concluded by the Council before the entry into force of the Lisbon Treaty, which would have given co-decisional power to the Parliament. the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (LIBE) affirmed that the agreement did not respect privacy rights, and recommended the rejection of the agreement when it finally was sent to the Parliament. Thus, the European Parliament rejected the interim SWIFT Agreement on February 11th, but a new round of negotiation soon started between the US and the EU. Indeed, the Commission manifested the interest in the conclusion of a new permanent agreement in a Recommendation to the Council. Thus, the EU and the USA opened negotiations on a new agreement that, this time, followed some of the Parliament suggestions. The revised SWIFT Agreement (SWIFT-II) was approved by the Parliament. A second rejection by the Parliament was very unlikely because of the importance for the EU to become a significant partner for the

USA in the field of counterterrorism. Still, SWIFT II was criticized by the European Data Protection Board and by part of the civil society.

The TFTP is a concrete example of the excessive monitoring activities of the United States, which have always been a cause of concern in the European Union and negatively affected bilateral relations. The Program, moreover, shows the different approaches of the US and the EU towards the value of privacy. The level of surveillance imposed by the TFTP did not raise as many concerns in the US as it did in the EU. Instead, the Program enjoyed the support and consensus of the American institutions. By contrast, the European Union had hard times in balancing the values of privacy and security in order to reach to a final agreement due to the high status of the right of privacy in Europe, and the resulting division within the European Union during the negotiations for the agreement. Moreover, while the SWIFT-II Agreement with the EU shows the multilateral approach that characterized the Obama administration, the TFTP is proof of the unilateralism of Bush administration, because of the secrecy that characterized the US initiative in spite of the existence of international means to cooperate against terrorism.

The fourth chapter is dedicated to an in-depth study of the legal frameworks on privacy and the regulations of personal data in the United Sates and the European Union. This analysis is important insofar as their different approaches to the right to privacy have a relevant effect on their cooperation on information sharing for security reasons.

The EU is the most protective regional framework for privacy. The case law of the European Court of Human Rights (ECtHR) regulates the legitimacy of state interference in the personal realm. According to the Court, states, in their activity to protect democracy, do not have an absolute power to monitor the individuals under their jurisdictions, especially if the measures that are adopted for monitoring activities may disrupt the democratic values they want to protect. This decision is particularly important because it really shows the regulatory approach to counterterrorism of the European Union discussed in the second chapter of this thesis. Although the EU is not bound by the ECtHR's decisions, the EU has a special consideration of the rulings of the ECtHR, as it considers them as establishing guidelines for the respect of human rights. The EU, indeed, is bound to access the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) after the entry into force of the Treaty of Lisbon in 2009, thus now bound by article 6 of the Treaty of the European Union. Moreover, the EU Charter of Fundamental Rights protects the ECHR regime in Art. 53. In 1981, the Council of Europe stipulated the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention N.108), which has the aim to conciliate the need for free circulation of information deriving from personal data and the need for privacy. Though the Convention is not a EU legal instrument, all EU members are parties to the Convention. Thus, Convention N.108 plays an important role in the European Union in the context of privacy protection. In 1995, the Data Protection Directive N. 95/46/CE was adopted by the European Parliament and the Council.

Originally, the Directive was conceived to build a common standard for the safeguard of personal data. The legal framework for privacy includes also the e-Privacy Directive 2002/58/EC, which regulates the use of and access to personal data of natural persons in the electronic communications sector, and establishes a central supervising and consulting body for the protection of privacy and personal data, namely the European Data Protection Supervisor (EDPS). The e-Privacy Directive was amended in 2006 by the so-called Data Retention Directive (Directive 2006/24/EC), which was conceived to harmonize the rules for the retention of personal data by electronic communications providers, in order to facilitate the investigation and prosecution of serious crimes. However, the Data Retention Directive was declared invalid by the European Court of Justice in 2014, for violating Articles 7 and 8 of the Charter. In 2012, the European Commission announced the possibility of reforming the European legislation concerning privacy. The aims were strengthening the protection of personal data as a fundamental right and creating new opportunities for the digital market. The legal framework for the protection of privacy now includes also Regulation (EU) 2016/679, which will replace Directive N. 95/46/CE on data protection; a Data Protection Officer introduced by the new Regulation; and Directive (EU) 2016/680 on the use of data by the authorities with the aim of prevention, investigation and criminalizing crimes or executing penal sanctions, which will replace Decision 2008/977/GAI of the Council.

Unlike the European Union, where the right to privacy enjoys the status of fundamental right, the US Constitution does not contain any express reference to privacy. However, some Amendments of the Constitution contain references that can be associated with various aspects of privacy. Thus, the protection of privacy is essentially based on rulings of the US Supreme Court, very specific federal laws and on a system of self-regulation. This should not suggest that privacy is not seen as a fundamental value in the United States. On the contrary, the United States contributed to the elaboration of international general guidelines on the protection of privacy. Moreover, even though the right to privacy is not expressly referred to in the Constitution, the Supreme Court of the US recognized the possibility for the federal states to guarantee higher levels of protection of privacy (Katz v. United States). As a consequence, many states started to develop their own legislations on privacy. However, this resulted in a very uneven framework for the protection of privacy, since the level of privacy protection may greatly vary between different states and significantly differ from the federal level. The only instrument at federal level that offers privacy protection and regulates the collection and use of personal data is the 1974 Privacy Act. The Act codifies the necessary principles for the collection and analysis of personal data. However, it is limited to certain specific fields. Moreover, until 2015, the Act applied only to US citizen, permanent residents, and foreign visitors. As it will be explained later, the 2015 Judicial Redress Bill, which extended the protection to EU citizens, marked a crucial shift in the bilateral negotiations on information sharing between the United States and the European Union. Other factors that influence the protection of privacy are that the US has no central supervising body, but rather various monitoring authorities (e.g. the Government Accountability Office). Moreover, privacy

authorities have been criticized for not being enough independent from the government. Consequently, the US lacks the sufficient oversight mechanisms that are necessary to ensure an effective protection of privacy. Not only does the US lack a substantial level of privacy protection at federal level, but also is not able to protect privacy rights that are guaranteed at international level, notably by the International Covenant on Civil and Political Rights (ICCPR). Though the US is a signatory state of the ICCPR, the United Nations Human Rights Committee has rated the US low on privacy protection.

Considering the observation present in the second chapter that regulation and oversight for the management of data are needed in order to guarantee the fragile balance between security and privacy within democracies, the fourth chapter describes also the role of courts, judges and data protection commissioners as monitoring bodies.

In the EU, judicial activities are crucial for protecting privacy in the European Union, both at European and at Member State levels. After the terrorist attacks of 2004 in Madrid and of 2005 in London, the European Parliament adopted the 2006/24/CE Directive on Data Retention, concerning the retention of data by communication services. Thanks to the concerns relating to privacy expressed by the MS, the ECJ found a violation of Articles 7 and 8 of the Charter of Fundamental Rights, which refer to the general protection of data and privacy. The European Court of Justice has a prominent role in defining the proper safeguards that are needed to retain data. Additionally, even national courts are playing a decisive role in the protection of privacy. In the EU, the courts are intervening also by limiting the power of intelligent agencies in the processing of personal data for security purposes. Moreover, the European courts are very active in the protection of privacy against non-European actors' violations, thereby protecting European standards on privacy (for instance, in Maximilliam Shrems v. Data Protection, the Court of Justice of the European Union invalidated the European Commission decision 2000/520/CE, which had accepted the level of privacy protection granted by the United States in the Safe Harbor regime). Lastly, the case of a proceeding started by the Belgian commissioner against Facebook is just one example of the active role of data protection commissioners within the European Union. Thus, not only is the EU characterized by a incredibly strict legal framework for privacy, but also by a very strong system of oversight thanks to the activities of European and national courts and other supervisory bodies.

After the terrorist attacks to the Twin Towers, the Congress of the United States passed the PATRIOT Act (2001), which expanded the monitoring powers of the government for the sake of national security. The PATRIOT Act was able to do so by amending every law regulating privacy, and was supported by the Congress. From that moment on, the surveillance activities of the American Government have been a major concern, especially with regard to the protection of personal data and privacy guaranteed to the US citizens. For being highly criticized, several pieces of legislation were passed in order to properly regulate the procedures for accessing personal data and protecting privacy in general (1974 Privacy Act, 1987 Computer

Security Act, etc). As far as criminal investigations are concerned, judges can issue orders that enables law enforcement authorities to monitor online communications in real time only if there are findings on a committed crime or on a crime that is being or is about to be committed. However, the major problem has been the incorrect interpretation of the PATRIOT Act by the government and its abuse of power. Moreover, concerning the access to stored data, the Electronic Communications Privacy Act (ECPA) does not even require a judicial approval.

The control that the United States has on its citizens is huge. Several times security agencies as the National Security Agency initiated secret programs for security purposes that had been discovered and denounced for their disregard of the law (e.g. leak of news on the TFTP). In 2006, the judgment of the federal judge Anna Diggs Taylor condemned the abuse of power of the Bush administration, and imposed the immediate interruption of the TFTP on the base of the violation of the First and Fourth Amendments of the USA Constitution. Other examples of surveillance are the Snowden revelation about the activities of the NSA, or the revelations on the NSA Prism Internet surveillance program. After the leak of news about the NSA spying operations, the United States' surveillance activities have been heavily criticized by the civil society but have also been a justification for other states to increase their level of surveillance. Within the USA, the Congress had to pass legislation to protect the right to privacy, but the legislation merely confirmed and legalized the practice of surveillance. In spite of the recently passed legislation, in 2015 another leak of news revealed the NSA wiretapping of European leaders. Mass surveillance increased in 2016 under the Trump administration. The Amendment of the Federal Rules of Criminal Procedures simplified the access to computers. Moreover, the appointments that characterized the American administration may further endanger the current status of protection of privacy, since the new administration seems to prefer national security requirements and emergency exceptions over human rights protection needs. All the above factors demonstrate the fact that the USA falls short of an adequate system of oversight of the intelligence, which has been criticized for recurring violations of the Constitution.

The numerous violations of privacy rights in the USA is inconsistent with the great influence of the Supreme Court on government activities. Despite its enormous powers, the Supreme Court, as well as the American judiciary branch in general, found themselves in a state of enduring contrast with the executive. A striking example is the recognition by the Supreme Court of the right to habeas corpus in various cases. However, the Military Commissions Act of 2006 passed by the Congress decided that the federal courts could not hear any more habeas corpus petitions filed by enemy combatants. The Act of 2006 was an attempt by the US Congress to bypass the decision of the Supreme Court for the enemy combatants detained in the military prison of Guantanamo. The Supreme Court declared the Act unconstitutional. Even though the US Supreme Court finally succeeded, this and other cases exemplify the contrast between the Congress and the Supreme Court concerning the respect of human rights and the abuses of the US government.

In sum, the comparison of the legal frameworks of the US and the EU concerning the protection of privacy, it is evident that the levels of privacy of the two actors are certainly different. Firstly, although privacy finds constitutional legitimacy in both the European Union and the United States, in the USA the creation of protections on grounds of privacy rests within the jurisprudence of the US Supreme Court. Secondly, the legislation of the EU treats the right to privacy as a general right, protecting all the categories that may fall within this right, notably the category of personal data. Instead, the USA have a sectorial approach towards the right to privacy, so its protection is not as extensive as the protection granted in the EU. Thirdly, in the European Union the courts perform a much more active role with respect to the United States as supervisory bodies. Fourthly, abuses of power and violations of the protection of personal data are very common in the United States.

Remarkably, the difference between the levels of protection of privacy in the US and the EU has slowed down the negotiations of agreements involving the right to privacy, as in the cases of the SWIFT and PNR agreements. Privacy concerns in the EU influence its propensity to accept international agreements that allow flows of information outside the boundaries of the EU. Following the terrorist attacks that involved some European states, a profound fear of terrorism generated claims for the share of more information, but at the same time many worries concerning the protection of privacy of EU citizens.

The EU-USA PNR Agreement embodies the struggle of the European Union to find a balance between privacy and security and the contrasts between the European Union and the United States to reach a final decision due to their different approaches to security and privacy. The expression Passenger Name Record (PNR) refers to personal data collected by airline companies following the booking of a ticket. After 9/11, the United States introduced a set of regulations that obliged airline companies to share the PNR information from all the planes departing from, in transit, or landing on the American soil with customs authorities. Thus, these disposition involved all the European airline companies that were subject to the European Directive 95/46/EC at the same time. Under the European Directive, the transfer of PNR data constituted an outflow of data towards a third party. For these situations, the European Directive did not allow the transfer of data towards countries outside the Union that couldn't guarantee the same level of protection of privacy. That marked the beginning of the controversy between the European Union and the United States. On the one side, the European Union wanted to ensure the protection of personal data of its citizens and the respect of national laws that had implemented the Directive. On the other side, even though the United States allowed for a delay of its new legislation about the PNR data to the month of March 2003, it provided that, from March, airline companies that couldn't respect the American legislation would have to be sanctioned. Thus, in 2003 the European Commission elaborated an interim agreement which, however, allowed the EU Member States to disregard Directive 96/45/EC. Negotiations between the EU and the USA about flows of PNR data started at the end of 2003 and were concluded only in 2012. It took 9 years before the two parties

reached a final decision. At this point, it is important to highlight some differences between the EU and the USA.

On the European side, negotiations with the United States started only after the decision of the US to systematically collect the entire massive amount of information on all the passengers flying to the US following the 9/11 terrorist attacks, because of major concerns that started to be raised within the European Union regarding the respect of the EU Data Protection Directive. However, some several control mechanisms that were put in place were quite fundamental for ensuring the protection of EU citizens' privacy. Indeed, the Parliament stepped in the negotiation process with the US numerous times requiring more safeguards for the protection of privacy. Moreover, during the 9 years of negotiations, when consensus seemed to be reached on the European side, either the European Court of Justice or the European Parliament intervened to invalidate the agreement and to criticize it on privacy protection grounds, respectively. While the European Union struggled to reach a final decision, the United States has always pushed for the finalization of the agreement. However, the reader should keep in mind that, as previously noticed in this chapter, the protection of privacy in the United States is extremely different than in Europe. As explained, the 1974 Privacy Act did not apply to EU citizens until 2015. The fact that the Act discriminated in protecting people has raised many concerns, notably when the US government initiated negotiations with the EU for the PNR Agreement.

As for the role of security in the negotiations, it is very enlightening to notice that the first version, namely the version with the lowest level of privacy guarantees (guarantees that were added after negotiations), has been approved after an increase in the perception of security threat in the EU. Indeed, it was approved by the Council right after the 2004 Madrid terrorist attacks, which caused an increase in the perception of threat. Indeed, the literature on risk-perceptions suggests that in the aftermath of a terrorist attack, people's fears condition the authorities to adopt emergency policies and new legislation to prevent similar tragedies. Those resolutions may be so extreme that could lead to a violation of fundamental law.

This case caused persisting disagreement within the EU. On the one hand, the agreement is considered as being extremely important because it is crucial for the intelligence to have information on the movement of people, especially considering the recent phenomenon of the foreign fighters. On the other hand, skepticism on the effectiveness of the PNR Agreement and critiques concerning privacy have been significant. For instance, in January 2015, in an intervention at the LIBE Commission, the European Data Protection Supervisor Giovanni Buttarelli heavily criticized the PNR system. In his speech, he admitted his skepticism towards the indiscriminate storage of data of the PNR, since he could not see how such a system could be useful to prevent terrorist attacks such as the Charlie Hebdo tragedy.

The last part of this thesis give conclusions on the role of privacy and security in EU-USA bilateral cooperation on information sharing and will try to put forward some recommendations and suggestions in the light of the findings.

First of all, the approval of the first version of the EU-US PNR agreement after terrorist attacks exemplifies the importance of considering the level of perception of security threat as the main boost for sharing information, thus being proof of the failure of the literature analyzed in the first chapter to recognize security as a cause of rather than a barrier to cross-border information exchange. Studies on the processes of international negotiations recognize that domestic interests play an important role, but no academic research investigates the role of domestic factors in international negotiation processes on the exchange of information. Secondly, it is clear that the EU and the USA do not guarantee the same level of protection of privacy. While security represents a boost for the progress of negotiations both at domestic (regional in the case of the European Union) and at EU-US level, the protection by the European Union of its legal environment represented a serious obstacle for the finalization of the PNR agreement. By contrast, a poor protection of privacy allows the US to focus more on security issues and push for negotiations for sharing information. Thus, a difference in the level of privacy can be considered as a barrier to the process of agreement-making on information sharing between the EU and the USA. Since the problem of the EU-US cooperation on information sharing for security purposes is the different level of privacy, one could wonder if harmonizing privacy protection could be a possible solution. However, absolute harmonization of legislation is unluckily. This is due to different reasons. Firstly, the cultural strategy of the USA makes politicians more prone to adopt questionable measures and justify them on grounds of national security. Secondly, EU and USA people attribute a different importance to the values of security and privacy. These reasons also make the idea of establishing international institutions or agencies for the exchange of information extremely complicated. A solution could be the creation of centers to exchange information about legal and regulatory solutions and methods of defense. Improving transparency would also be an optimal strategy, because it would increase the level of trust in law enforcement authorities. As many scholars suggest, the use of secrecy in measures that are resorted to combat terrorism may have a negative impact on rights. Thus, cross-border information sharing is certainly a huge step towards a counterterrorism regime based on a more effective protection of rights, and it is important to continue to cooperate in this sense. Constitutional law has greatly improved in addressing problems that are due to the excessive use of secrecy by executive powers. Indeed, the increasing interaction between legislative and judicial branches, and between national and supranational regimes ensures a more effective observance of constitutional values. As for the United States, it is clear that it lacks proper supervision over the activities of the intelligence. Thus, independent oversight bodies and some control mechanisms should be established in order to firstly, guarantee the protection of the privacy of US citizens, and secondly, increase its credibility as an international actor in the protection of fundamental rights and international treaties. More generally

speaking, this thesis encourages further research in this area in order to better fill the current gap in the literature on the roles of security and privacy and their influence on processes of data exchange.