L.L.M. International and European law

Faculty of Law

Tilburg University, The Netherlands

Counterterrorism, a threat to data protection?

June 2017

Student: **Aline Havaux**

ANR: 648765

Supervisor: **Dr. Nikolas M. Rajkovic**

Table of contents

List of abbreviations

American Civil Liberties Union	ACLU
European Union	EU
European Convention on Human Rights	ECHR
Foreign Intelligence Surveillance Act	FISA
FISA Amendment Act of 2008	FAA
Foreign Intelligence Surveillance Amendment Act	FISAA
Foreign Intelligence Surveillance Court	FISC
International Covenant on Civil and Political Rights	ICCPR
Non-Governmental Organisation	NGO
Office of the High Commissioner for Human Rights	OHCHR
Organisation for Economic Cooperation and Development	OECD
United Nations	UN
Universal Declaration of Human rights	UDHR
United Nations' General Assembly	UNGA
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act	USA PATRIOT Act
U.S. National Security Agency	NSA

Introduction

Since the terrorist attacks committed in the United States on 11 September 2011, the approaches towards national security have significantly changed. Three main reasons explain these changes: first, the new attitude regarding terrorism, second, the development in technologies and, more especially, in communication technologies, and third, the globalization. Since these attacks, the number of terrorist attacks has constantly risen and with it, we observe an increase of counter-terrorism measures. One of them is the creation of national databases, which collect, analyse and store personal data and information about individuals. Governments have developed more and more global mass surveillance systems that collect information not only upon European and American citizens, but also on every individual that might interest the security and intelligence services. In fact, we can discern a common trend whereby the communications and online behaviour of the very large majority of citizens are monitored by governments. We also observe that data mining and sharing are increasingly used to prevent terrorist attacks. Those pre-emptive counterterrorism powers aim to identify individuals who might commit terrorist crimes in order to enable the investigators to prevent those individuals to perpetrate terrorist-related activities[1].

Those measures have a great impact on human rights, especially on the right to privacy and to data protection, which are now very vulnerable. Though the privacy problems are not as important as the questions of torture or the right to life, it remains that the intrusion into the private sphere of innocent people all around the world has significantly increased these past few years[2]. According to C. Wilka, "*A data breach means there is a loss, theft, or unauthorized access to someone's confidential personal information contained in electronic data*"[3]. Therefore, we observe a tension between the right to privacy (and to data protection) on the one hand and, on the other hand, the right to security. Also, the absence of a legal definition of "terrorism" at the international level leads states to interpret terrorism broadly,

---

1 K. LACHMAYER, "Rethinking privacy beyond borders – Developing transnational rights on data privacy", *Tilburg Law Review*, 2015, p. 93; D. LOWE, "Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty", *Terrorism and Political Violence*, 2016, p. 668; A. VEDASCHI A. and V. LUBELLO, "Data retention and its implications for the fundamental right to privacy", *Tilburg Law Review*, 2015, p. 15.

2 K. LACHMAYER, *o.c.,* p. 93; A. VEDASCHI A. and V. LUBELLO, *o.c*., p. 15.

3 C. WILKA, "The effects of *Clapper v. Amnesty International USA*: An improper tightening of the requirement for article III standing in medical data breach litigation", *Creighton Law Review*, 2016, p. 477.

which also raises questions regarding the circumstances in which the data of the individuals can be used. There is a clear risk of abuse of this data information for other purposes than the fight against terrorism.

Legally speaking, some rights are considered as more important than others and so, some rights need to restrict other rights in order to be fulfilled. The right to security might be one of them. Indeed, it seems that governments pay more attention to security than to data protection. But, on the other side, some authors[4] have put forward the assumption that maybe terrorism arises because of a lack of human rights protection. Others[5] have suggested to redefine the notion of "privacy". This research will assess that redefining is not a good solution to resolve the tension between the right to security and the right to data protection. Indeed, by reducing the standard of data protection, we do not resolve the issue. Rather, this research will argue that a solution to protect the right to privacy of individuals is to develop more rights for individuals regarding the right to data protection and privacy.

Moreover, over the past years we saw the emergence of several criminological and legal writings dealing with the impact that terrorism has had on democratic states and individual rights and focusing on "*how recent terrorist acts have legitimised states' illiberal legislative and policy responses to the terrorist threat they face resulting in a rights-based democracy being replaced by a "siege mode of democracy"*"[6]. According to some authors, the fear of terrorism led to the creation of neo-democracies where seemingly liberty, security, and fundamental freedoms are respected but, in reality, are only available to the few. Following this view, governments use terrorism as an excuse to extend the core element of counterterrorism to cover all sorts of conducts that do not fall into most people's perception of terrorism. This can lead to the introduction of quasi-criminal law provisions that have the appearance of freedom but only on the surface and not in substance[7]. Indeed, as observed by A. Dreher and M. Gassebner, there is a clear link between terrorism in human rights and that governments tend to restrict human rights as a response to terrorism[8]. Since the 9/11 attacks,

---

4 See A. DREHER, M. GASSEBNER and L.-H. SIEMERS, "Does terrorism threaten human rights? Evidence from panel data", *The Journal of Law and Economics*, 2010, pp. 65-93.

5 See P. ROSENZWEIG, "Privacy and counter-terrorism: the pervasiveness of data", *Case Western Reserve Journal of International Law*, Vol. 42, Issue 3 (2010), pp. 625-646.

6 D. LOWE, *o.c.,* p. 659.

7 D. LOWE, *o.c.,* p. 659 referencing to C. GEARTY, *Liberty & Security,* Cambridge, Cambridge: Polity Press, 2012, pp. 55-56 .

8 A. DREHER, M. GASSEBNER and L.-H. SIEMERS*, o.c.,* pp. 65-94.

we indeed observe a strain on individuals' rights with the increase in the adoption of authoritarian powers to policing agencies to restrain the liberty of individuals considered as a terrorist threat in order to avoid a terrorist attack before it occurs[9]. Therefore, this research will focus on the question to know whether the counterterrorism measures adopted by governments threaten the human rights, and more especially the right to data protection. Other questions also arise, such as the question to know whether those measures to fight the terrorism are compatible with human rights, and more particularly with the right to data protection. It also raises the question to know to what extent the fight against terrorism justifies the override of the right to data protection.

The use of data information by governments has been even more questioned in the last few years, especially since the revelations of Edward Snowden, a former United States National Security Agency (NSA). Indeed, those revelations showed a whole new dimension and quality of surveillance by the states but also international cooperation between states and between states and private sectors. Especially, the NSA has collected information regarding emails and data files, etc., that have important implications in terms of right to privacy and data protection of citizens. Their purpose is to obtain as much information as possible about the greatest amount of people. It resulted in a condemnation by privacy activists of the widespread surveillance practices and the mass collection of data or communications of ordinary individuals used by counterterrorism agencies and raised the question to know how states' counterterrorism legislations have permitted those agencies to impede to such an extent on individuals' liberty. Indeed, although governments' officials justify those infringements of privacy as a necessary mean to prevent terrorism, it has been argued that those measures create an inhibiting surveillance climate and reduce basic freedoms. This question of the protection of data privacy has become increasingly important in public discussion in liberal democracies[10].

This problem of dataveillance is particularly touchy in the United States (U.S.), particularly after all those revelations regarding the information of millions of U.S. customers collected by the NSA. Even before that, some cases have been brought to the Court, including *Clapper v.*

---

9 D. LOWE, *o.c.,* p. 659 referencing to H. FENWICK, "Proactive Counter-Terrorism Strategies in Conflict with Human Rights", *International Review of Law, Computers & Technology,* 2008, pp. 259-260.

10 K. LACHMAYER, *o.c.,* pp. 93-94; D. LOWE, *o.c.,* p. 653; M. MILANOVIC, "Human rights treaties and foreign surveillance: privacy in the digital age", *Harvard International Law Journal*, 2015, p. 81; A. VEDASCHI A. and V. LUBELLO, *o.c.,* pp. 15-16.

Amnesty International where the respondents claimed that the state had bypassed the Fourth Amendment[11]. The Court decided to dismiss the respondent's claim, arguing that it's purely speculative but this decision was subjected to a lot of critics from human rights lawyers and groups. After Snowden's revelations, two others important cases were brought (*Klayman v. Obama* and *American Civil Liberties Union v. James R. Clapper*) before respectively the U.S. District Court for the District of Columbia and before the U.S. District Court of Southern district of New York. In the *Klayman* decision, Judge Leon relied on *Clapper* decision to say that, contrary to *Clapper*, there was strong evidence that the data had been collected. In the *American Civil Liberties Union* decision, Judge Pauley interestingly took an opposite view by saying that there is no evidence that the data had been collected for any other purpose than investigating and disrupting terrorist attacks. Those two latest decisions illustrate the divisions in the American body politic following Snowden's revelations and the complexity that those counterterrorism terrorism mechanisms raise regarding the right to data privacy.

As shown, the tension between the right to data protection and the right to be protected from terrorist attacks is more and more preeminent. It appears that privacy and non-discrimination rights are being challenged by the increased surveillance and profiling of suspected terrorists. Indeed, this research argues that the fight against terrorism tends to go beyond its purpose and to override on human rights. Some protection mechanisms are put into place by governments' policies to safeguard the right to data protection but the question arose to know if there are really effective and sufficient. The compatibility of those measures with constitutions and human rights has easily been raised before courts all over the world, especially in United States. This research will demonstrate that it seems that the governments have lost the balance between those two rights, especially since there is a risk that the governments will use the excuse of counterterrorism to use the personal information collected on individuals for other purposes. Furthermore, one may wonder if the measures such as data surveillance, data mining and profiling are really helpful to prevent terrorist attacks. Some reserves may be expressed in that regard. Therefore, this research will acknowledge that those measures put an important strain on human rights and that it's not certain whether there are efficient security measures. Furthermore, it raises serious questions about their value. As a result, this work will

---

11 U.S. Constitution Amendment IV: "*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*".

analyse how governments and courts are handling the balance between privacy and terrorism and why the governments do not respect this balance anymore. Since the governments do not seem close to change their strategy regarding counterterrorism, Courts should counterbalance this lack of consideration for privacy by putting human rights back at the centre of the debate.

This thesis will examine the mechanisms put into place by the governments regarding personal data to fight terrorism. Besides, it will analyse how those mechanisms are implemented and their legality and compatibility with human rights, more particularly the right to data protection recognized by article 12 of the Universal Declaration of Human Rights and by article 17 of the International Covenant on Civil and Political Rights. It will also examine the ways in which the governments and courts are justifying the overriding of the right to data protection.

In order to answer the questions raised, Chapter I of this research will first analyse if and how the countermeasures to fight against terrorism put into place by the governments constitute a threat to the right to data protection and to what extent. In that regard, this work will first examine the use of the new technologies by terrorist organisations and, after the international instruments and mechanisms found to fight terrorism. The second chapter will be dedicated to the consideration of the overriding of the data protection rights as a means to deal with the threat to data protection. To address this issue, this research will first attempt to define terrorism and then discuss the right to data protection. Finally, the final chapter will illustrate those considerations by showing how the U.S. deal with the threat of terrorism. In that regard, this work will examine the *Clapper v. Amnesty International* case but also the most recent *Klayman v. Obama* and *American Civil Liberties Union v. Clapper* cases.

Chapter I: A threat to data protection?

The world we live in has been completely changed these past few years by the technological developments and revolution in communication. As a consequence of those evolutions, the nature of our inter-personal interactions has been profoundly transformed. However, on the other side, those transformations have also considerably affected our human rights. Indeed, on the one hand, the digital revolution has offered new ways to protect fundamental rights and liberties as they have improved global access to information, encouraged freedom of expression, and endorsed civic engagement. Nevertheless, on the other hand, innovations in communication technology have raised new questions regarding the protection of human rights, especially the right to data privacy. Furthermore, terrorist networks have found in the digital evolution a fertile terrain to spread their ideology. At the same time, governments and private companies have seen in communication technologies a great instrument to monitor individuals and collect data on their behaviour. In the context of terrorism and counterterrorism, this is not without consequences on the protection of privacy and personal data[12].

In order to fight terrorism, governments have rightfully emphasized prevention of terrorist attacks (among other means such as criminal law for instance) rather than reaction. Indeed, prevention reduces the risks carried by individuals. In order to prevent terrorist acts, counter-terrorist operations need information[13].

I. Use of new technologies by terrorist organisations

The last 20 years, the Internet has developed considerably. Therefore, it's not surprising that law enforcement agencies pay more and more attention to the use of the Internet for criminal purposes, notably by suspected terrorists. Indeed, it is well established that terrorist groups use the Internet "*for communication, propaganda, research, planning, publicity, fundraising and creating a distributed sense of community*"[14].

---

12 F. FABBRINI, "Privacy and national security in the digital age – European and comparative constitutional perspectives", *Tilburg Law Review*, 2015, pp. 5-6; W. N. RENKE, "Who controls the past now controls the future: counter-terrorism, data mining and privacy", *Alberta Law Review*, 2006, p. 780.

13 W. N. RENKE, *o.c.,* pp. 780-784.

14 I. BROWN and D. KORFF, "Terrorism and the Proportionality of Internet Surveillance", *European Journal of Criminology*, 2009, pp. 119-121.

Indeed, the Internet provides a social networking function to terrorism as it allows terrorists to normalize their behaviour and develop a sense of persecution. Moreover, the Internet also changed the way terrorism works: groups can now be geographically dispersed and non-hierarchical. Furthermore, the new technologies provide new opportunities for the terrorists to collect information and disturb intelligence agencies' operations [15].

II. International instruments and mechanisms to fight the terrorism regarding personal data: surveillance, profiling and data sharing

In order to respond to the terrorist threat, policing and intelligence agencies have put into place different policies that have an impact on the right to privacy of the Internet users who have no connection with terrorism or serious crime, such as surveillance, data sharing and profiling. Indeed, the development in communications technology enabled the improvement of computing capability and data storage capacity. Those measures put nevertheless an important strain on human rights[16]. Thus, profiling is a technique often used that consists in linking the criteria with the characteristics based on personal experience or shared experience of individuals. Of course, it is not because one individual satisfies the criteria that he or her will have the characteristic (of a terrorist)[17].

We observe that national governments and supranational organisations make great use of the technological developments to increase their capacity to locate individuals, intercept their communications and target them. They do that, either directly taking on the surveillance task through empowerment of intelligence or law enforcement agencies that are in charge of monitoring and intercepting electronic communications or, by delegating this surveillance task to the private sector, for instance by asking internet service providers and telephone companies to store metadata about electronic communications for a certain number of years and put them at the disposition of the police or secret services if needed[18]. Whatever the method used by governments, this is a great violation on individuals' privacy and it creates an inhibiting surveillance climate. Furthermore, there is no guarantee that this information will not be used in other contexts than counterterrorism. Without any guarantee and considering the great impact of those measures on basic freedoms, it seems that the governments have lost

---

15 I. BROWN and D. KORFF, *o.c.*, p. 122; W. N. RENKE, *o.c.,* p. 783.
16 I. BROWN and D. KORFF, *o.c.,* pp. 120 and 123; H. FENWICK, *o.c.,* p. 259.
17 W. N. RENKE, *o.c.,* pp. 792-794.
18 F. FABBRINI, *o.c.,* pp. 6-7.

the balance in the protection of the right to privacy on one hand, and on the other of the right to security.

A. Data mining as an intelligence source

With the recent and growing security concerns raised by terrorism, data mining has been used as a mean to acquire information. Its utility as a source of information is based on a series of facts. Data mining is seen as a suitable way to fight terrorism but it has to be governed responsibly or the costs might exceed its benefits. Indeed, data mining has important benefits but it can also engender severe risks of its own (see *infra*. Chapter II, II, C.)[19].

The idea underlying the use of data mining to prevent terrorist attacks is based on the hypothesis that if terrorists plan an attack, their operatives will engage in transactions that will produce electronic records. Therefore, data mining is seen as a useful tool to detect terrorist signature. The early identification of the terrorist signature will allow the detection of terrorist activities and to take the appropriate counterterrorism measures. Unless they engage only in cash transactions, the non-obvious characteristic of those patterns will make it very difficult for terrorists to engage into counter-surveillance tactics as they will not know which patterns to avoid[20].

Data mining is made possible by the significant advances in computer-related technology. As a result, the private sector and governments have established large electronic holdings about individuals and their transactions. Not only is the information stored in records, but it is also organized and analysed. That is where "data mining" comes into the picture[21]. Besides observing, an algorithm used by surveillance computers allows the identification of "targets" and police and other authorities focus their attention on them[22]. Although this method has its benefits in terms of speed, there is also a risk of error and of targeting innocents. If that is the case, not only does it have grave consequences on the individuals wrongly targeted but also, it focuses the attention of the police and other intervention teams on the wrong suspects, allowing the terrorists to lead their activities without being monitored.

---

19 W. N. RENKE, *o.c.,* pp. 779-780 and 785.
20 *Ibid*., p. 788.
21 *Ibid*., pp. 785-786.
22 I. BROWN and D. KORFF, *o.c.,* p. 123.

Originally, the term "data mining" means "*searches for one or more electronic databases of information*"[23]. This broad meaning includes two types of procedures: query based information recuperation and automated pattern discovery. While query based information recuperation divulges information "*that is already expressly or explicitly in a database or set of databases*"[24], automated pattern discovery is the "*nontrivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data*"[25]. The difference between the two resides in the fact that the latter does not reveal information that is expressly in the database or databases analysed. The search patterns are detected by means of algorithms applied to training data[26].

As established by I. Brown and D. Korff,

> New surveillance technologies exploiting these capabilities include mechanisms to monitor, screen and analyse records of billions of telephone and email communications; 'bugs' and tracing technologies that can access the geographical position of mobile phones and act as a remote listening device; and hard-to-detect (even with anti-virus tools) 'spyware', surreptitiously installed on a suspect's computer by the authorities, that can remotely and secretly monitor a suspect's online activities, passwords and email, and even the computer's camera and microphone[27].

Data mining is therefore very intrusive as it involves searches through the personal information of many individuals. For that reason, it is a big interference with privacy interests. Furthermore, there is a risk that individuals may be wrongly inculpated in the investigative process. One way to reduce this interference in privacy by data mining is to use selective revelation. Indeed, technology permits to recourse to such techniques where the information given to the analysts is first in a "sanitized form" that does not reveal the identity of the subject. It is a form of "security barrier" between the individual and the analyst. It is only if the information is considered as significant that it will be brought to the attention of

---

23 Report of the Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* (Washington, D.C., March 2004), online: Center for Democracy and Technology, https://www.cdt.org/files/security/usapatriot/20040300tapac.pdf (consulted on 1st June 2017), p. viii.

24 W. N. RENKE, *o.c.,* p. 786.

25 U. FAYYAD, G. PIATETSKY-SHAPIRO, P. SMYTH, "From Data Mining to Knowledge Discovery in Databases", *Al Magazine*, 1996, pp. 40-41.

26 W. N. RENKE, *o.c.,* p. 786.

27 I. BROWN and D. KORFF, *o.c.*, p. 123.

analysts. In this way, we have the assurance that most information will not fall into government officials' hands. Moreover, if an application and a court order are required to link the information to the identifiable individuals, it is an additional assurance that only the information that is needed for the state will be given to the state[28].

The data mining method has several aims: the collection of information relevant to preserve national security and, more particularly, the collection of information allowing the identification of terrorists, to provide aid in their prosecution and, last but not least, to detect terrorist threats and prevent terrorism actions from occurring. In order to fulfil these tasks, some wrongly argue that there should be a relaxation or decline of constitutional standards as counterterrorist operations have to act as fast as possible to prevent attacks from occurring. The respect of constitutional procedures applying to ordinary law enforcement is a luxury that counterterrorism cannot afford. On the other hand, others rightly say that it is precisely because there is a lot at stake that it requires being cautious. Indeed, once an individual is identified as being a terrorist or being involved in a terrorist plot, the consequences are swift and devastating. And if that individual has been wrongly targeted, it is the state itself that inflicted that great injury. In addition, it diverted the attention of the state on the actual terrorists, leaving the nation vulnerable. Therefore, this research argues that data mining should be subjected to scrupulous procedures instead of sloppy procedures. In that regard, W. N. Renke rightly considers that instead of diminishing procedural rigour when it comes to data mining, there should be constitutional procedures. Indeed, constitutional procedures are not obstacles but, rather, they confirm and empower good investigative and enforcement work as they require the state to provide solid reasons to use coercive and often violent measures. However, it is true that, in some circumstances, particular steps in counterterrorism operations may require fast intervention that does not accommodate usual procedures. That said, we should recall that the mere existence of terrorist risks does not, by itself, constitute an emergency. It is only when serious risks reach the point of imminence or when risks are in the process of actualisation that we can talk about emergencies[29].

A safeguard that has been settled is that before resorting to data mining, the applicant will have to explain why data mining is needed in order to obtain the authorisation to use data mining. Indeed, data mining is a highly suspect operation and, in order to demonstrate that the

---

28 W. N. RENKE, *o.c.*, pp. 813-815.
29 *Ibid.*, pp. 811-812.

limitations to privacy caused by data mining are justified, the applicant should be required to demonstrate that data mining is likely to be effective for the generation of reliable results[30]. Considering the potential drawbacks of data mining, one may however wonder if it is a sufficient safeguard to privacy.

Due to the monitoring of the "data trails" left by the individuals in many transactions and to the accessibility of communications databases that contain such trails, a commensurate expansion in "dataveillance" has been observed. Those data are detained for a certain period of time and include telephone numbers dialled and emails senders and recipients (but not the content of those calls and messages). Moreover, the rules that govern the access to communications data and on data retention are opaque and unable to guarantee that the data of innocent individuals will not be collected and held by law enforcement authorities, or used for "profiling". Rather, those surveillance programs have been designed to spy on individuals' action on a global scale. Therefore, data mining does not only breach the privacy of the few terrorists among us but breaches the privacy of every individual that have disclosed information that may be mined. All this data provides an extremely detailed portrait of an individual. In this context, little room is left for privacy, especially when state investigators can see with whom individuals communicated, what they read and watch online and where they travel via the use of their mobile phone[31]. In the light of these considerations, the question of the proportionality can be raised. Indeed, it does not seem proportionate that the information of each individual is collected and analysed whereas there are only few terrorists among us. In this context, each individual gives up (most of the time unconsciously) his rights to privacy to protect others from terrorist attacks. Therefore, it is obvious that governments give priority to security over privacy and lost the balance between those two rights.

At the European level, the data collected is also meant to be shared across Europe due to the principle of "availability", as mentioned in the "Hague Programme". Under this principle, data sharing and free access is given to the data collected, without any of the usual obstacles included in the traditional instruments for transnational cooperation between law enforcement agencies. Indeed, European law enforcement agencies now commonly use "profiles" created, not by any one national police force but, rather, as part of the international cooperation to target suspects. In order to facilitate targeted searches on potential terrorists depending on the

---

30 *Ibid*., p. 816.

31 I. BROWN and D. KORFF, *o.c.*, pp. 123-124; F. FABBRINI, *o.c.*, p. 8; W. N. RENKE, *o.c.*, p. 809.

member states, information is collected on residents, foreigners, university students and similar information sources. This data is later matched to physical, psychological or behavioural characteristics that the law enforcement agencies think present a high probability of terrorist activity. Not only do the police and intelligence agencies use this data resources in order to find previously identified suspects for specific offences (terrorists or other), but they also exploit them in order to match all those databases against a pre-determined profile that is dynamically updated. Moreover, those searches are based on secret, unchallengeable information that are implemented as part of European policies. Another problem of these programs is that they are based on built-in biases of which even software producers are often unaware of and that only appear when the programs are actually used in practice but only if their functioning is appropriately monitored to identify such distortions[32]. Furthermore, most of the surveillance programs have been designed and carried out in secret, without a close examination[33].

Due to the growing cooperation between intelligence and law enforcement agencies at national and international level, the data collected through surveillance programs are also increasingly shared across the world. This international cooperation allowed governments to bypass the constitutional safeguards on the privacy of citizens as they have recourse to the support of foreign authorities to conduct unlawful surveillance on their own nationals[34].

Obviously, many of those technologies are not without consequences on individuals' privacy as they allow the state to have an extremely close control over its citizens' lives. Therefore, although profiling and data mining seem to work up to a certain point, I. Brown and D. Korff rightly assess that it leads to actions against a very large number of innocent people on a scale that is unacceptable in a democratic society[35].

In the light of the above, it seems clear that governments have lost the balance between the right to privacy and the right to security, putting the right to security first and permitting important abuse on the right to privacy of the individuals (whose most of them are innocents). Therefore, those measures don't seem proportionate to ensure the security. Moreover, the

---

32 I. BROWN and D. KORFF, *o.c.*, pp. 124-125; F. FABBRINI, *o.c.,* pp. 8-9.
33 F. FABBRINI, *o.c.,* p. 8.
34 *Ibid*., pp. 8-9.
35 I. BROWN and D. KORFF, *o.c.*, p. 125.

collection and storage of this information would be an even greater attempt on basic freedoms and fundamental rights of individuals if those data were to be used in another context than the fight against terrorism.

B. Instrument of prevention against terrorists' attacks

We talk about instrument of *prevention* because in the area of terrorism, "*the aim is to prevent* possible *crimes by people who* may *commit them*"[36]. The instruments of prevention against terrorists' attacks are driven by the development in communications technology.

A problem with those instruments of prevention is that there are generally directed against individuals deemed to be suspicious on the grounds of certain stereotypes or due to their affiliation to a specific group. Therefore, there are higher chances that they lead to discrimination against such minority groups[37]. However, those discriminations are not considered as an unconstitutional offence and courts have held that there is no constitutional harm when law enforcement agencies use public behavioural traits to target people as potentially dangerous as long as they do not only rely on immutable characteristics such as race or gender[38].

---

36 *Ibid*., p. 126.

37 *Ibid*., p. 127.

38 See e.g., *Whren v. United States*, 517 U.S. 806, 813 (1996); *United States v. Brigoni-Ponce*, 422 U.S. 873, 885-887 (1975); ROSEN, "The naked crowd: Balancing privacy and security in an age of terror", *Arizona Law Review*, 2004, p. 617.

Chapter II: Overriding of the data protection rights as a way to deal with the threat

I. Terrorism: attempt of a legal definition

At the present time, there is still no unanimous definition of what constitute "terrorism". However, despite its lack of international definition, it is generally admitted that terrorism possesses several characteristics. Indeed, it is characterised by the important violence it exercises. This violence can manifest through different means such as propagating a sense of fear to achieve a determined political outcome, put pressure on a government to change its policy, mediate the ideology of a program or organization to bring in new members, etc. Furthermore, terrorist acts vary from acts of resistance by the fact that they are directed against civilian populations. Civilians are in fact only indirect objectives that influence the decisions of political leaders. Moreover, terrorism must be distinguished from guerrilla warfare by the fact that it is based on psychological influence, whereas guerrilla warfare focuses on the physical control of a territory. But overall, what seems to distinguish terrorism more from other forms of war is the fact that it systematically violates international laws of the law of war[39].

The term "terrorism" has to be used with caution as it is often used in an abusive way in order to discredit a person or to justify the resort to force[40]. For this reason, there is reason to fear that the governments will use the notion of terrorism to justify the multiple abuses to the right to privacy of individuals, even in circumstances that do not fall into most people's perception of terrorism. This kind of conduct is inacceptable in democratic societies and show the importance to have an international agreement on what terrorism constitutes. Otherwise, it can lead to abuses and to undermine basic fundamental rights, including the right to privacy.

---

39 K. BAYRAMZADEH, "Les Etats faillis et le terrorisme transnational", *Rev. Dr. Ulg*, 2015, pp. 104-105 ; I. BROWN and D. KORFF, *o.c.*, p. 126; P. CURRAT, "Le droit face à de nouvelles générations de guerre et de terrorisme", *Revue de l'avocat*, 2016, pp. 103-105.

40 K. BAYRAMZADEH, *o.c.,* p. 103.

II. Right to data protection

A. Data protection as a fundamental right

Although national security is a legitimate concern and the duty of states and supranational institutions is to protect individuals from terrorist attacks, this omnipresent surveillance has raised a lot of concern about the protection of the rights to privacy and to the protection of personal data. These two rights are indeed protected in both national constitutions and international human rights treaties[41].

The right to privacy relates to the right to respect private life and is recognised as a fundamental right by article 12 of the Universal Declaration of Human Rights (UDHR) and by article 17 of the International Covenant on Civil and Political Rights (ICCPR). The right to data protection "*is not only concerned with protecting individuals from intrusions into their privacy or private life, but more broadly against the improper collecting, storing, sharing and use of data*"[42]. However, it seems that the protection encounters the problem of the definition of "privacy" not only at the domestic, but also at the international level. And even if it is possible to define privacy in an incomplete and partial way that will be subjected to refinement and continuous critique, the questions remain to know whether this notion should be contained by such definition and what role should be played by a human rights approach in that regard. Indeed, human rights law might be useful as regards to the challenge of giving privacy content and ensure its protection. Another way to picture privacy is to see it as a protection that involves the consumer's education and vigilance when they set their own privacy controls online[43]. Despite the debate about the question to know whether privacy finds its roots in conceptions of either liberty, or dignity, legal scholars agree that the idea that privacy must at least protect the intimate sphere from interference by public authorities[44]. Some argued in favour of a "pragmatic privacy" regarding mass surveillance where the focus is not put on the collection of data but rather on the use, oversight and transparency of the process[45].

---

41 F. FABBRINI, *o.c.,* p. 7.
42 I. BROWN and D. KORFF, *o.c.,* p. 120.
43 D. JOYCE, "Privacy in the digital era: human rights online?", *Melbourne Journal of International Law*, 2015, pp. 11-12.
44 F. FABBRINI, *o.c.,* p. 8.
45 D. JOYCE, *o.c.*, p. 12.

The conceptual confusion regarding the scope and content of the privacy protection and technological advances is not without consequences since it limits the privacy protection. On the other side, both factors lead us to consider more deeply the necessity for further development on international privacy law and to give a greater attention to the project of digital rights translation[46].

Regarding the right to data privacy, the question can be raised to know who deserves privacy. Indeed, in the U.S. it is largely admitted that citizenship is the basis for fundamental rights. Moreover, the public debate generally considers that only citizens have constitutional rights, whereas foreigners do not. For that reason, non-citizens enjoy fewer protections than citizens. It is therefore not surprising that some of the most far-reaching surveillance programs conducted by the NSA and authorised under Section 702 of the Foreign Intelligence Surveillance Act (FISA) explicitly narrow the scope of their application to prevent surveillance of any individual known to be located in the U.S., and of any U.S. citizen or permanent resident reasonably supposed to be located outside of the U.S. Thus, non-U.S. citizens and permanent residents are only protected against surveillance when they are on the U.S. soil. As a result, both the physical presence of an individual on the U.S. territory and his or her citizenship or residence status are relevant with regards to the enjoyment of the right to privacy for the FISA's drafters[47].

Whereas the U.S. polity was in the process of deciding whether fundamental rights should be grounded in citizenship, this choice has already been made in the international human rights system. Indeed, by definition, the human rights are universal, they are granted to all humans by the mere fact that they possess inherent dignity that deserves protection. Therefore, the question whether individuals enjoy human rights, and more especially the right to privacy, *vis-à-vis* a particular state should not depend on the question whether they have the nationality of that state. It does not mean however that no distinction may be drawn at all on the basis of other characteristics of the target such as his or her location, the type of surveillance or his or her individual features. For those reasons, this research argues that citizens and non-citizens should be granted the same protection of their rights generally, and of privacy specifically.

---

46 D. JOYCE, *o.c.*, p. 12.
47 M. MILANOVIC, *o.c.,* pp. 88-89.

Indeed, in the counterterrorism and surveillance context, there is no reason to believe that non-citizens pose a greater threat to a state's security than its citizens[48].

It is worth repeating that states have the positive obligation to secure and ensure the respect of human rights and protect the individuals within their jurisdiction against human rights violation by third parties. This positive obligation implies first the regulation by the states of "*private companies operating in areas under control that collect, store, process, or have access to personal data*"[49]. Second, it implies that the prevention of interferences with privacy by third parties need to be exercised by states with due diligence and in taking into account all the effective measures reasonably available to them. A further difficulty arises when a state engages in surveillance of its population and then shares the information collected to a third party. To deal with those issues, some authors, such as M. Milanovic, rightly point out that human rights treaties apply to foreign surveillance activities[50].

That being said, we must remember that most human rights, including the right to privacy, may be restricted in their application when objectively justified by the circumstances. In that regard, one may note the difference in the interpretation of "private life" and "correspondence" between the European Court and the U.S. Supreme Court. Indeed, whereas the European Court has interpreted those concepts very generously and, thereby, has increased the scope of acts that constitute a violation of privacy, the U.S. Supreme Court has interpreted the notions of search and seizure more narrowly because it was the only way to avoid what seemed to be a too rigorous and strict requirement for a specific search warrant on probable cause. As a consequence, the scope of the right to privacy is wider under the European Court of Human Right than under the current state of the U.S. Supreme Court doctrine on "reasonable expectations of privacy". Accordingly, the human rights framework is inherently flexible as regard the justification of interferences with privacy but, at the same time, it is very inclusive on what constitutes such interference. However, one should keep in mind that even though the human rights framework can be applied in a more flexible way, it must not be applied so flexibly that it would be deprived of any impact or would compromise the integrity of the whole regime. We therefore find ourselves faced with a paradox where the current arrangements adopted by the governments run the risk to be found unjustified within

---

48 *Ibid*., pp. 97-101.
49 *Ibid*., p. 123.
50 *Ibid*., pp. 123-124 and 129.

the human rights framework but, at the same time, the proponents of the protection of privacy run the risk that these arrangements can be found acceptable within the very same framework. This paradox is intensified as the relevant courts or treaty bodies operated their review differently. At the end of the day, even if the human rights framework is flexible, it still has an impact on the existing surveillance practices. M. Milanovic considers in that regard that "*there is room enough within the human rights framework for both meaningful privacy protections and effective intelligence work*"[51].

The differences in the interpretation of the term "privacy" in Europe and U.S. show the complexity of the challenges we face now. Those different approaches lead to uncertainty and, consequently, to insecurity, not only regarding the right to privacy but also regarding national security. Therefore, this research argues in favour of the adoption by the international community of a binding regulation to have a common understanding of the current problem that counterterrorism poses to privacy, and data protection particularly. As the next section will show, there already exist international regulations to address this challenge but it is very fragmented and non-binding. Nevertheless, it has the advantage of bringing this question to the international scene.

In the context of terrorism and counterterrorism, it appears that there is an urgent need for establishing and strengthening international data privacy rights. In order to address all different issues of data privacy in the context of transnational surveillance, there is a necessity for the development of a more detailed concept of international digital rights. Indeed, one may notice that although intelligence agencies and police cooperation are already working together at the international level, the protection of data privacy is not organised at the global level in the same way[52].

B. Standards and Regulations

In order to address the problem of global surveillance properly, there is a need to develop international tools that supplement domestic and regional approaches regarding privacy. When addressing the problem of data privacy at the international level, we have to take

---

51 *Ibid*., pp. 131-132 and 139-140.
52 K. LACHMAYER, *o.c.,* p. 78.

different perspectives into account such as "*the international dimension of surveillance, the limits of institutional control by the states themselves and the effectiveness of data privacy*"[53].

In order to address properly the international dimension of state surveillance, international standards on data privacy are necessary. Some international standards already exist and provide transnational principles and rights regarding data privacy, such as the UDHR, the ICCPR, the European Convention on Human Rights (ECHR), the Organisation for Economic Cooperation and Development (OECD) Guidelines, the Council of Europe, etc. For instance, the Council of Europe provides for two conventions: the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and the Cybercrime Convention (Convention 185). Despite the fact that these two conventions are not applicable to intelligence agencies, they are part of the international data protection framework and can be used as international references for data protection. Nevertheless, in order to apply these treaties to state surveillance, their scope needs to be extended explicitly. More economic-focused approaches have also been adopted, notably the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data but they exclude the question of national security[54].

There are a lot of uncertainties regarding the application of human rights treaties to intelligence gathering. Indeed, it is inevitable that the legality of electronic surveillance programs will be challenged by human rights language and forums. Moreover, the special rapporteurs of the UN Human Rights Council already have started to analyse the impacts that the counterterrorism measures may have on the right to privacy[55].

A major development in that regard is the UN General Assembly (GA) Resolution 68/167 on "The Right to Privacy in the Digital Age" adopted on 18th December 2013 under the sponsorship of Brazil and Germany. This resolution constitutes an important step towards the protection of privacy in the digital era and at the international level. Indeed, it brings the issue of electronic surveillance within the framework of international human rights law. Furthermore, it invokes both Article 12 UDHR and Article 17 ICCPR. Although the focus of this resolution is put on privacy in the digital age, it can also be seen as a reproach from the

---

53 *Ibid*., pp. 97-98.
54 *Ibid*., pp. 98-99.
55 M. MILANOVIC, *o.c.,* p. 83.

international community after Snowden's revelations (see *infra.* Chapter III, II, B). Like GA's resolutions, the tone is rather neutral but it reflects nevertheless the significant political move to focus attention to the kind of privacy-intrusive mass surveillance due to the internet and digital media environment[56]. This resolution could nevertheless be a starting point for other initiatives towards an international treaty on data protection[57].

In the Preamble, the Assembly expresses its deep concern

> at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights[58].

The resolution 68/167 first acknowledges that on one side, the technological development enables the individuals to use new information and communication but, on the other side, it "*enhances the capacity of the governments, companies and individuals to undertake surveillance, interception and data collection*", which can result in human rights violations[59].

This resolution illustrates the future approach to privacy protection in the sense that it affirms the relevance of "*the analogy of privacy to new contexts such as the internet and mass digital surveillance*"[60]. Although this aspect is persuasive, more needs to be done to understand the problems faced in digital translation rights and to appreciate new contexts. Indeed, the right to privacy should be applied online and also in relation to mass surveillance[61]. In that regard, the resolution calls upon states to

> (a) To respect and protect the right to privacy, including in the context of digital communication;

---

56 F. FABBRINI, *o.c.,* p. 9; D. JOYCE, *o.c.,* p. 2; M. MILANOVIC, *o.c.,* p. 85.

57 K. LACHMAYER, *o.c.,* p. 100.

58 *The Right to Privacy in the Digital Age*, GA Res 68/167, UN GAOR, 3rd Comm, 68th sess, 70th plen mtg, Agenda Item 69(b), UN Doc A/RES/68/167 (21 January 2014, adopted 18 December 2013 ("Resolution 68/167"), Preamble, § 10.

59 *The Right to Privacy in the Digital Age*, GA Res 68/167, UN GAOR, 3rd Comm, 68th sess, 70th plen mtg, Agenda Item 69(b), UN Doc A/RES/68/167 (21 January 2014, adopted 18 December 2013 (hereafter "Resolution 68/167"), Preamble, § 4.

60 D. JOYCE, *o.c.,* p. 5.

61 *Ibid*.

(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law[62].

If we look at the resolution 68/167 as a whole, it is unclear whether if offers something new regarding digital privacy in order to develop privacy norms and address the difficulties encountered[63].

Overall, the most important aspect of this resolution is that it opens a process, a dialogue, "*on the application of human rights norms to surveillance, interception, and data collection activities, even when such activities are conducted by a state outside its borders*"[64].

In June 2014, the Office of the High Commissioner for Human Rights (OHCHR) adopted a report on privacy in the digital age. In this report, the OHCHR recognized at the same time that the advances on information communication technology are powerful and offered the promise of improved human rights enjoyment but also that these new technologies are vulnerable to electronic surveillance and interception. Such surveillance is a threat to individuals' rights, including the right to privacy, and prevent the free functioning of a dynamic civil society[65]. Although this report is very much in favour of the protection of the privacy, it acknowledges the legitimate national security interests of the states without putting the right to privacy on a pedestal of human rights fundamentalism[66]. Notably, the report correctly recognises that the interferences with the privacy of electronic communications cannot be justified by the fact that "*individuals voluntarily surrender information about themselves and their relationships in return for digital access to goods, services and information*"[67], that the collection of communications metadata is as much intrusive as the collection of the content of the communications since "'*metadata' may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication*"[68], and that, due to

---

62 Resolution 68/167, § 4.
63 D. JOYCE, *o.c.,* p. 5.
64 M. MILANOVIC, *o.c.,* p. 85.
65 Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the OHCHR*, U.N. Doc. A/HRC/27/37, 30th June 2014 (hereafter "OHCHR Report").
66 M. MILANOVIC, *o.c.,* p. 143.
67 OHCHR Report, § 18.
68 OHCHR Report, § 19.

the chilling effect of surveillance, that "*[t]he very existence of a mass surveillance programme […] creates an interference with privacy*"[69]. Therefore, the report expresses a broad understanding of what constitutes an interference with privacy[70].

As mentioned earlier, a certain degree of interference in some human rights is authorised. In that regard, the report interprets the text of Article 17 ICCPR according to which interferences with privacy are only justified when they are not arbitrary and unlawful, meaning when it is legal, necessary and proportionate[71]. The Report accepts that national security is a legitimate interest to justify interferences with privacy but, however, "*[t]he degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose*"[72]. What poses particularly serious problems with regard to mass surveillance is the proportionality grounds. Indeed, the report notes that

> [w]here there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is *both necessary and proportionate* to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate[73].

It is not so much the bulk collection that poses a problem in itself but rather the vast scale, magnitude, and relative permanence of certain mass surveillance programs that raise proportionality concerns[74].

In the report, the OHCHR also expresses its concerns regarding mandatory third-party data retention policies and considers that intelligence and data-sharing arrangements may violate

---

69 OHCHR Report, § 20.
70 M. MILANOVIC, *o.c.,* p. 143.
71 OHCHR Report, §§ 21-23; M. MILANOVIC, *o.c.,* p. 143.
72 OHCHR Report, § 24.
73 OHCHR Report, § 25.
74 M. MILANOVIC, *o.c.,* p. 144.

the right to privacy[75]. In regards to the distinctions made in domestic legislations regulating surveillance based on the nationality of the individuals, the report criticizes this approach and addresses the importance of the involvement of private actors in governmental surveillance[76]. The report ends with a series of recommendations, and the most important one expresses that

> there is a clear and pressing need for vigilance in ensuring the compliance of any surveillance policy or practice with international human rights law, including the right to privacy, through the development of effective safeguards against abuses. As an immediate measure, States should review their own national laws, policies and practices to ensure full conformity with international human rights law[77].

Following the OHCHR report, the GA revisited this issue and adopted another resolution on this subject: Resolution 69/166 on "The Right to Privacy in the Digital Age" which further illustrates the debate over digital privacy in the General Assembly context and strengthens the earlier Resolution 68/167. Resolution 69/166 acknowledges the role that the human rights framework can play regarding the problem and specific concerns of metadata and unlawful surveillance of digital communications. However, and although it draws on the analysis of the OHCHR Report, this resolution still does not go as far as some would like. In its report, the OHCHR recognises that mass surveillance may violate privacy and that the states have to justify such interference in a transparent and on-going manner[78].

Also, some scholars rightly declare that it is undeniable that human rights treaties apply to the vast majority, if not all, of foreign surveillance activities, including the bulk collection of communications and personal data of a great amount of ordinary people. This is precisely the case due to the fact that surveillance measures are now used on a lot of ordinary people both at home and abroad, instead of only on the agents of foreign governments. As a consequence, the question arises to know whether there is an extraterritorial right to privacy. The answer to that question will obviously differ: while some will argue in favour of more protection for privacy both internally and externally, others will incline towards the pursuit of national security interests. Again, we see that the two rights are in balance and that one of them will

---

75 OHCHR Report, §§ 26-27; M. MILANOVIC, *o.c.,* p. 144.
76 OHCHR Report, § 45.
77 OHCHR Report, § 50.
78 D. JOYCE, *o.c.,* pp. 6 and 9-10.

count more heavily in the balance, depending on the approach adopted. Therefore, on one side we have the proponents of privacy that will argue that any distinction between individuals based on their citizenship and immigration status should be abandoned, that bulk collection and mass surveillance are violations of the right to privacy and are disproportionate, that the judicial supervision is an important safeguard against those abuses, that the individuals that are subjected to surveillance should have a right to be notified after the fact, and that states have positive obligations to prevent spying by third states and to regulate private actors. On the other side, governments with extensive surveillance programs will rebut all or some of these arguments but some states might be more disposed to accept them. In that context, the human rights law will provide a space where contestation at the international legal level can take place and where those issues can be rationally discussed. In this regard, it is worth noting that there is a follow-up process to the General Assembly's privacy in the digital age resolution. Furthermore, the human rights implications of foreign surveillance are now on the agenda of national parliaments and other deliberative bodies. Moreover, the Human Rights Committee and other treaty bodies conduct periodic review of state reports. It is in that context that the Committee examined the U.S. fourth periodic report in March 2014 and expressed its serious concerns about the NSA's surveillance programs and noted that the U.S. should[79]

> take all necessary measures to ensure that its surveillance activities, *both within and outside the United States,* conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity *regardless of the nationality or location* of individuals whose communications are under direct surveillance[80].

Foreign surveillance is also subjected to review before the Human Rights Council, as well as the Council's special procedures. For this purpose, a special rapporteur on privacy has been established for the first time in July 2015 for three years[81]. Finally, as it will be examined in

---

79 M. MILANOVIC, *o.c.,* pp. 140-142.

80 U.N. Human Rights Comm., Concluding Observations on the Fourth Report of the United States of America, advance unedited version, March 2014, p. 9, available at http://justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf (consulted on 8th June 2017).

81 Office of the High Commissioner for Human Rights, Special rapporteur on the right to privacy, available at http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx (consulted on 8th June 2017).

more details in the last chapter, there are more and more litigations brought by individuals and NGOs that challenge the surveillance measures, before both domestic and international courts[82].

To sum up, we observe a fragmented structure of an international data privacy framework at the international level. Furthermore, next to the general international framework, there are also different forms of principles and rights provided at the international level, especially by soft law. Yet, state surveillance is not included in the scope of the international data privacy framework. In order to improve the protection of personal data in the fields of police authorities and intelligence agencies, there is a need to develop and amend the existing international treaties but also the jurisdiction of international human rights courts and bodies. The international human rights catalogues refer explicitly to privacy as a human rights and can thus be considered as good approach. Nevertheless, certain human rights can be derogated from and the national security will always be a legitimate justification to restrict individuals' privacy[83]. Therefore, there is a need to find a good balance between the right to privacy on the one hand and, on the other hand, the right to security. Although the right to security is highly important, further safeguards should be adopted in order to protect the privacy of the individuals as much as possible.

Two contrasting views are adopted regarding the role of human rights in the digital age. Thus, in a provocative and largely critical contribution, F. Johns emphasises both the limitations of human rights law at a conceptual and practical level when it comes to the challenge of the digital environment and big data[84]. In that regard, she raises the question to know if it might "*be time to re-think our preoccupation with privacy and associated icons, such as the consenting data subject*"[85]? F. Johns "*contends that there is much more at issue in the governance of the emerging global data economy than technical interface between existing legal systems and well-aired privacy concerns*"[86]. Furthermore, this scholar explores the different ways in which personal data and privacy concerns "*tend to enshrine an integrated, wilful, relatively self-contained personhood even as they sketch a technological and communicative context in which that personhood is but a contingent assemblage of strewn*

---

82 M. MILANOVIC, *o.c.,* p. 142.
83 K. LACHMAYER, *o.c.,* pp. 100-101.
84 F. JOHNS, "The deluge", *London Review of International Law*, 2013, pp. 9-34; D. JOYCE, *o.c.,* pp. 15-16.
85 F. JOHNS, *o.c.,* p. 27.
86 *Ibid*., p. 14.

bits"[87]. According to her, the notion of privacy is incapable to render or address actual and potential problems encountered by people engaged in the global data economy. F. Johns considers that the limitations of a digital privacy approach, and of a traditional institutional response, have to be examined further and she advocates considering the complexity of the contexts before returning to "the routine characterisations of law" such as an individual's right to privacy[88]. This view is quite pessimist. Rather, this research argues that the human rights offers a possibility to protect privacy and security both at the same time, but it has to be re-thought and adapted to the actual world, taking into account the actual and potential technological developments.

For his part, M. Milanovic takes a contrasted view as regard the suitability of a privacy framework in emergent digital contexts. Indeed, according to him privacy law can address the situation we are facing now. He rightly highlights that litigants already use the right to privacy and the developments in relation to digital privacy to argue in human rights terms that mass surveillance is unlawful, that it violates privacy and that a further jurisprudential development can contribute to overcome doctrinal challenges such as the extraterritorial application of human rights. In that regard, he properly highlights that the Assembly's resolution on the right to privacy in the digital age is a major development because it brings the issue of electronic surveillance within the framework of the international human rights law[89]. M. Milanovic advocates that "*human rights should apply to virtually all foreign surveillance activities*"[90]. As successfully expressed by this author, an international human rights law approach prevents discrimination in terms of treatment of individuals in different states. Besides, as the author notes "*this is precisely where the universalist normative foundation of human rights comes in: an interpretation which values all human beings equally and is respectful of their individual dignity is inherently more preferable than one that does not*"[91]. Unfortunately, M. Milanovic does not address the deeper question to know whether international human rights law assures equality of outcome and experience of the law[92].

---

87 *Ibid*., p. 25.
88 F. JOHNS, *o.c.,* pp. 26 and 34; D. JOYCE, *o.c.,* p. 15.
89 D. JOYCE, *o.c.,* p. 13; M. MILANOVIC, *o.c.,*, pp. 81-86.
90 M. MILANOVIC, *o.c.,* p. 87.
91 *Ibid*., pp. 109-110.
92 D. JOYCE, *o.c.,* p. 14.

When it comes to the development of international rights on data privacy, K. Lachmayer properly assesses in his contribution that we need to go beyond a general right to data protection but rather, that we should provide more particular rights to individuals. Indeed, a general right to privacy would be a starting point to handle the challenges regarding data privacy caused by counterterrorism measures by states. But, since there are various elements of data privacy, different rights are needed to address all the aspects of privacy in the information society. In that regard, a possibility would be to inform individuals after a certain a period of time that they have been subjected to surveillance. Another possibility relies on the fact that several digital rights can be developed from a fundamental right to self-determination of the use of personal data such as a right to be informed, a right to access to the information, a right to rectify or delete and a right to object. Incidentally, it will allow individuals not only to start judicial review but also to control state surveillance. Indeed, as rightly pointed out by this scholar, the establishment of principles regarding data privacy is useful to define certain standards for state authorities but it does not bind those authorities. For this reason, it is essential to give certain rights to the individuals. Indeed, the empowerment of individuals is an important part of data privacy and is accompanied with different important rights such as the right to be informed by public authority after the data collection, the right to receive an answer when the public authority is asked about the personal data detained or the possibility to go to court in case of rejection of information. It is thus important that the substantive rights of data privacy are combined with certain procedural rights and access to an independent court in order to create the basis for effective legal protection[93].

Obviously, it is foreseeable that electronic surveillance and related activities will remain on the agenda of the UN bodies for the upcoming years. The discussion has just started and it is expected that it will concentrate on human rights by focusing on the rights and interests of the affected individuals, and not only on the interests and sovereignty of states. Indeed, each individual deserves some protection of his privacy, not because two states agreed not to spy on each other's citizens, but because of the equal and inherent human dignity of all individuals[94].

---

93 K. LACHMAYER, *o.c.,* p. 98 and 101.
94 M. MILANOVIC, *o.c.,* p. 86.

C. The risks of data mining and profiling

As already demonstrated, the use of data mining is a useful tool when it comes to the prevention of terrorist attacks and counterterrorism measures. However, it comes with its potential costs, especially as it involves violation of privacy[95]. The violation of the right to privacy of innocent individuals in national security is quite significant and not without consequences[96]. Indeed, since the revelations of the systematic practices of governments and agencies to collect personal data of individuals, the protection of the right to privacy has been put under great pressure in the name of the fight against terrorism.

The very essence of data mining is to seek out personal information or information about individuals. Indeed, if it was unable to link identifiable individuals, it would be pointless in assisting in identifying terrorists and in preventing terrorist attacks. On the other side, when individuals provide information to private, public non-governmental, or governmental custodians, they assume that the information will only be used for the purposes for which it was collected. Data mining is problematic as it acquires the information, analyses it and produces information that may be used by governments for counterterrorism purposes, without the consent of the individuals or their notification. Those violations in individuals' privacy are justified by the fact that data mining can be used to prevent terrorist attacks. In order to constraint the risks triggered, data mining has to face three main types of challenge. First, there must be a reasonable judgement that data mining will actually deliver the benefits promised. Second, the risks produced by data mining must not outweigh any benefits it may deliver. Third, the limitation to other valuable interests (such as privacy) must be necessary to achieve the objectives of data mining[97].

As previously mentioned, an important drawback of the profiling technique to identify potential terrorists is that it is based on bias or prejudice of human-generated profiles. Those bias and prejudice may be buried deeply in code[98]. This can be seen as a discrimination of individuals as it will lead to target certain groups of people, which generally, are minority groups in societies. If such is the case, it would be a violation of article 7 of the UDHR and article 26 of the ICCPR.

---

95 W. N. RENKE, *o.c.,* p. 790.
96 K. LACHMAYER, *o.c.,* p. 80.
97 W. N. RENKE, *o.c.,* pp. 790-791.
98 *Ibid*., p. 794.

Furthermore, profiling has error rates ("false positives" and "false negatives"), depending on the reliability of the criteria and their application. Those error rates in profiling create complications when it comes to data mining as the latter deals with large data sets and large populations. Indeed, innocent individuals might be wrongly targeted as a result of a small percentage of false positives (individuals who possess the criteria but do not have the characteristic). Therefore, it may be extremely difficult to develop reliable profiles for terrorists. Additionally, terrorists' conduct before an attack is meant to appear legitimate. Moreover, there are poor chances that the types of terrorist attacks that have already occurred will be repeated as terrorists have a large scope for innovation. For these reasons, some authors argue that in addition to the development of profiles on known terrorist conduct, profiles should also take into account events frequently correlated with terrorism, "*such as illegal immigration large funds transfers, the use of front business and recruitment activities*"[99].

A first risk inherent to data mining rests on the weaknesses that undermine its capacity to provide useful and precise intelligence or, alternately, that it can provide erroneous information. These weaknesses stem from the fact that data mining rely on recorded information and from its use to obtain intelligence from records. It is however possible that the data may be incomplete, incorrect, incomprehensible and/or inconsistent. Furthermore, even when data is recorded accurately and properly, the use of different formatting standards and different databases may make data sharing difficult[100]. Those drawbacks are inacceptable in a democratic society. Indeed, no one can doubt that data mining is a useful and powerful tool in the fight against terrorism but its costs should not exceed its benefits. Indeed, if the data collected is, for instance, incorrect, it could lead to serious prejudices on the individual wrongfully targeted. Admittedly, the national and international security are important but it should not be used as an excuse to infringe others human rights in such a strong way.

Thereupon, an important risk with data mining lies in the fact that the technique could fail to provide reliable information. If that is the case, there will be individual costs and there will be a threat on national security. Indeed, the state will wrongly target individuals that are innocent and that will suffer the imposition of severe burdens. Moreover, it will also affect people

---

99 *Ibid*., pp. 792-794.
100 *Ibid*., pp. 791-792.

connected to the wrongly targeted individual. This data mining inaccuracy is an important threat to national security as it focuses attention on the wrong individuals and, therefore, take the attention of human and technological resources away from other inquiries and investigations, thus allowing terrorists to work freely[101].

Another risk generated by data mining concerns its misuse. Indeed, if data mining is used outside of the contexts in which it is justified or if it is used without authorisation, it would be a considerable abuse. This risk is a real and important one as data mining has been deployed as an extraordinary tool to address the special needs of counterterrorism. But, it is reasonably argued that state officials will inevitably use data mining also for other offences than terrorism. Moreover, the information collected through data mining could be made public inappropriately and could be abused if authorised users do not protect properly the confidentiality or if third parties managed to obtain unauthorised access to the system or system records. Another possibility is that the authorised users abuse data mining capabilities to perform searches and reveal results for illegitimate purposes. Sadly, this last possibility is not only theoretical since there have already been cases[102].

Furthermore, even if there are not misused, there are some inherent social, political and personal risks in data mining methods. Since access to personal information of individuals is given to the state for law enforcement purposes on the basis of "individualised suspicion", pattern-based data mining threatens the relationship between individuals and the state. Pattern-based data mining implies that the state has a broad access to many individuals' personal information, which allows it to develop profiles and to challenge those profiles with that information when there is no evidence for even a suspicion of a wrongdoing. Therefore, the state intrudes in individuals' private lives like never before, which constitutes a great abuse to individual liberty and is against limitations of state power. The consequences of these violations of individuals' rights cannot be properly predicted now but there is a clear risk that a "chilling effect" will occur and that the individuals will constrain their freedoms of belief, expression or association to not fall under the suspicious patterns[103].

---

101 *Ibid*., p. 795.
102 *Ibid*., p. 795.
103 *Ibid*., pp. 796-797.

Moreover, whether the person poses a real or fictitious threat to the security, the persons concerned by data mining are usually not aware of it and have no possibility to get access to the personal data held by intelligence agencies[104]. Although we understand the obvious need for intelligence and security agencies to keep this information secret to accomplish successfully their operations, it nevertheless constitutes a problem regarding the right to privacy. Maybe a solution could be to give access to the information collected and stored after a certain period of time. Therefore, more rights need to be given to individuals at the international level.

Furthermore, the international data sharing that increases with counterterrorism measures, makes it even more complicated for the persons concerned by data sharing to obtain access to their information retained. The sharing of this information depends on the different agencies that grant the approval for those exchanges. For this reason, the transnational data exchange needs to be accompanied by an adequate development to enable data protection rights beyond borders. Another problem regarding the international exchange of counterterrorism information is that the mechanisms aimed at protecting the data often depend on the national legislation of the relevant countries. But, in any case, the persons concerned do not know that their personal data are subjected to such exchanges. Yet, it can have significant effects on innocent individuals, especially in the context of the fight against the terrorism. Furthermore, if those personal data were to be used in another context, one can imagine the great abuse of the right to privacy that would occur[105].

For all those reasons, this research assesses that there is a need to rethink privacy in a broader sense that will go beyond borders from a right-based perspective. In addition, in order to have an effective legal control of data exchange in the context of terrorism, the individuals need to have rights to be aware that their data has been processed and to have a legal review from an independent authority or court[106].

---

104 K. LACHMAYER, *o.c.,* p. 80.
105 *Ibid*., pp. 80-81.
106 *Ibid*., p. 81.

Chapter III: Surveillance powers and counterterrorism in the United States

I. U.S. powers

For state's counterterrorism agencies to operate, it is important for them to work within the rule of law. Not only does it ensure that their practices respect the principle of proportionality but it also allows for transparency[107]. Unlike in the European Union, there is no explicit constitutional right to data privacy in the U.S. Therefore, the case law of the U.S. Supreme Court developed a rights-based approach regarding the right to privacy based on the U.S. Bill of Rights, especially the Fourth and First Amendment[108].

Regarding the U.S., there are two significant statutes that authorize electronic surveillance. The first statute granting for electronic surveillance is Section 2516(1) Title 18 United States Code, which allows for covert surveillance in order to obtain "*intelligence on terrorist-related activity when the Attorney General authorises a Federal judge to grant a Federal agency an order to intercept wire or oral or electronic communications*"[109].

The second one is the Foreign Intelligence Surveillance Act 1978 (FISA) according to which a Federal agency, with Attorney General approval, applies to a Foreign Intelligence Surveillance Court "*for an authority to conduct electronic surveillance on 'agents of foreign powers', including persons suspected to be engaged in international terrorism*"[110]. FISA regulates various electronic surveillance of communications that are used by the federal government for foreign intelligence aims. The statute calls for the procurement of warrants or court orders by the government for certain foreign intelligence surveillance activities. Two specialised courts were therefore created to assist the progress of such surveillance[111]. First, the Foreign Intelligence Surveillance Court (FISC) in charge of approving electronic surveillance if there is plausible reason to believe that "*the target of the electronic surveillance is a foreign power or an agent of a foreign power*" and that "*each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used,*

---

107 D. LOWE, *o.c.,* p. 654.
108 K. LACHMAYER, *o.c.,* p. 94.
109 D. LOWE, *o.c.,* p. 654.
110 *Ibid*., p. 654.
111 J. M. MASTRACCI, "*Klayman v. Obama*: The D.C. District Court misinterprets the NSA metadata collection program as a violation of individual Fourth Amendment rights", *Tulane Journal of Technology and Intellectual Property*, 2014, p. 367; X. "Standing – Challenges to Government Surveillance – *Clapper v. Amnesty International USA*", *Harvard Law Review*, 2013, p. 299.

by a foreign power or an agent of a foreign power"[112]. Second, the Foreign Intelligence Surveillance Court of Review that may review FISC "*denials of applications for electronic surveillance*"[113].

When Section 702 of the FISA, which is directed against non-U.S. individuals located outside U.S. territory, was discussed, the President's Review Group emphasized the need to safeguard the legitimate privacy interests of foreigners, while justifying at the same time the distinctions drawn by the FISA in those terms[114]:

> FISA's especially strict limitations on government surveillance of United States persons reflects not only a respect for individual privacy, but also-and fundamentally a deep concern about potential government abuse *within our own political system.* The special protections for United States persons must therefore be understood as a crucial safeguard of democratic accountability and effective self-governance within the American political system. In light of that history and those concerns, there is good reason for every nation to enact *special* restrictions on government surveillance of those persons who participate directly in its own system of self-governance[115].

However, this reasoning is not persuasive. The surveillance of ordinary people on a mass scale is certainly prejudicial to any free and democratic society but it cannot be used as a justification to draw categorical distinctions between citizens (or permanent residents) and foreigners. Indeed, the privacy interests of the latter are no less worthy of protection[116]. In this regard, the Review group noted that "*there are sound, indeed, compelling reasons to treat the citizens of other nations with dignity and respect*"[117]. Furthermore, the Review Group directly invoked the Universal Declaration of Human Rights and the International Covenant on Civil

---

112 U.S. Code, Title 50, § 1805 (a) (2) (A)-(B).

113 X. "Standing – Challenges to Government Surveillance – *Clapper v. Amnesty International USA*", *o.c.*, p. 299.

114 M. MILANOVIC, *o.c.*, p. 95.

115 The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World", 12 December 2013**,** p. 154, available at https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (consulted on 6th June 2017).

116 M. MILANOVIC, *o.c.*, p. 95.

117 The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World", 12 December 2013**,** p. 155, available at https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (consulted on 6th June 2017).

and Political Rights in the foreign surveillance context[118]. In addition, in his response to the Review Group's report, President Obama declared that "*people around the world, regardless of their nationality, should know that the United States is not spying on ordinary people who don't threaten [their] national security, and that [the United States] take their privacy concerns into account in [their] policies and procedures. This applies to foreign leaders as well*"[119].

Following its adoption, FISA has been expanded several times. In 1999 a new section (Title V) was introduced to permit access to certain business records for foreign intelligence and international terrorism investigation. This section was further expanded after September 11, 2001, domestic terrorist attacks and consecutive to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) legislation[120]. The latter completely replaced the Title V and authorized access to business records in "*investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the [First Amendment]*"[121]. However, in 2006 the Congress narrowed this provision by requesting reasonable grounds to believe that the tangible things sought are pertinent regarding the prevention of international terrorism or clandestine intelligence activities[122].

In 2008, important changes were brought to the NSA's electronic surveillance powers through the Foreign Intelligence Surveillance Amendment Act (FISAA). This amendment authorises surveillance on non-U.S. citizens outside U.S. territory, which means that the personal data of those citizens is now under the range of U.S. jurisdiction. This is not without consequence since while U.S. citizens located in the U.S. have knowledge of their right to privacy under the Fourth Amendment, no such right is applicable to foreign citizens[123]. In that regard, we should remember that the Fourth Amendment provides individuals "*the right […] to be in*

---

118 *Ibid.*

119 B. OBAMA, President of the United States, Remarks by the President on Review of Signals Intelligence, 17th January 2014, available at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence (consulted on 6th June 2017).

120 J. M. MASTRACCI, *o.c.,* p. 367.

121 Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 501(a)(1), 115 Stat. 287 (2001).

122 U.S. Code, Title 50, §1861; USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 (2001); J. M. MASTRACCI, *o.c.,* pp. 367-368.

123 D. LOWE, *o.c.*, p. 654; X. "Standing – Challenges to Government Surveillance – *Clapper v. Amnesty International USA*", *o.c.,* p. 299.

their persons, houses, papers, and effects, against unreasonable searches and seizures"[124]. Furthermore, unlike FISA was originally drafted, under the 2008 amendment, the government is not required to demonstrate credible cause that a target is a foreign power nor is it required to designate the nature and location of each "*of the particular facilities or places at which the electronic surveillance will occur*"[125].

On the day FISAA was adopted, numerous attorneys and human rights labour, legal and media organisations started a lawsuit in order to obtain the recognition that this amendment violates the Fourth and First Amendments, article III and the separation of powers principles, and to obtain the interdiction of its use[126].

Regardless of the absence of an explicit right to privacy in the U.S. Constitution, the U.S. Supreme court has developed certain guarantees against the surveillance by the state. This approach adopted by the Supreme Court is nevertheless limited and faces restrictions, such as the exclusive protection of the U.S. citizens. Instead of promoting privacy the last decade, the U.S. Congress choose to focus on the counterterrorism. As a consequence, while privacy was not protected effectively, personal data has become more and more easily accessible for intelligence agencies. Nevertheless, recent developments such as the U.S. Freedom Act reveal a change of the U.S. Parliament towards more limitations of the intelligence agencies' activities, but it remains uncertain whether the rights of individuals with regards to data privacy will be reinforced by the legislator at the same time[127].

II. The *Snowden* affair and its implications regarding legal decisions

In June 2013, a huge media outcry was triggered after Snowden's revelation to a *Guardian* journalist, Glenn Greenwald, regarding the NSA and Prism program that gave U.S. Federal agencies direct access to servers of big web firms such as Google, Microsoft, Facebook, Yahoo, Skype and Apple. Snowden also issued top-secret documents that revealed that a top-secret order issued in April 2013 allowed the NSA to collect records of millions U.S.

---

124 U.S. Constitution Amendment IV.

125 X. "Standing – Challenges to Government Surveillance – *Clapper v. Amnesty International USA*", *o.c.,* p. 299.

126 *Ibid*., pp. 299-300.

127 K. LACHMAYER, *o.c.,* pp. 94-95.

customers[128], adding that those communication records are collected "*indiscriminately and in bulk regardless of whether they are suspected of any wrongdoing*"[129]. According to Greenwald, this shows how NSA's mission has changed from being exclusively devoted to foreign intelligence gathering to one that focuses increasingly now on domestic communications[130]. Those revelations had a significant political fallout as they revealed the sheer technological capacity of the NSA and of the other intelligence agencies to collect personal data on a very large scale and to intercept Internet communications[131].

After Snowden's revelations, a declassification of the United States Foreign Intelligence Surveillance Court (FISC) revealed that telephone metadata collection was supported by a foreign intelligence surveillance statute which had authorised the access to business records for foreign intelligence and international terrorism investigations in accordance with the USA PATRIOT Act[132]. Snowden's revelations were accompanied by a renewal interest in privacy as a human right[133]. The question then arose to know if the program used by the NSA is constitutional under the First and Fourth Amendments to the United States Constitution[134].

The fact that NSA actions were posing a threat to the privacy of EU citizens worried the EU's Justice and Home Affairs Council, so that the EU's Justice Commissioner Vivian Reding stated that:

> The European Commission is concerned about the possible consequences on EU citizens' privacy. The Commission has raised this systematically in its dialogue with the U.S. authorities, especially in the context of the negotiations of the EU-U.S. data protection agreement in the field of police and judicial co-operation […][135].

---

128 E. E. CONNARE, "*ACLU v. Clapper*: The Fourth Amendment in the Digital Age", *Buffalo Law Review*, 2015, pp. 395-396; D. LOWE, *o.c.*, p. 656; J. M. MASTRACCI, *o.c.,*, p. 365; M. MILANOVIC, *o.c.,* p. 81.

129 G. GREENWALD, "NSA Collecting Phone Records of Millions of Verizon Customers Daily", *The Guardian*, June 6, 2013, available at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (accessed on March, 30th 2017).

130 *Ibid*.

131 M. MILANOVIC, *o.c.,*, p. 82.

132 J. M. MASTRACCI, *o.c.,* p. 365.

133 D. JOYCE, *o.c.,* pp. 1-2.

134 M. RAPISARDA, "Privacy, technology, and surveillance: NSA bulk collection and the end of the *Smith v. Maryland* era", *Gonzaga Law Review*, 2015/16, p. 124.

135 N. WATT, "PRISM Scandal: European Commission to Seek Privacy Guarantees from U.S.", *The Guardian*, June 10, 2013, http://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees (accessed on March, 30th 2017).

During this dialogue, the difference in legal culture between the EU and the U.S. regarding individuals' right in respective jurisdictions was striking. Indeed, while the EU requires a system of protection of individual citizens' data privacy, such an explicit protection does not exist under the U.S. Bill of Rights, rather it can be deduced from the First, Fourth, Fifth and Ninth Amendments. It is relevant because Snowden's revelations have not only the potential to damage diplomatic relations between the U.S. and the EU, but may also affect the "*terrorism intelligence-sharing between the European counter-terrorism agencies via Europol and U.S. federal agencies*"[136].

A. Court decision pre-Snowden: *Clapper v. Amnesty International*

Clapper v. Amnesty International is a good example that demonstrates how national security can override individuals' liberty provisions in U.S. anti-terrorism law. In this case, the U.S. Supreme Court had to examine the FISAA amendments to section 702 FISA and the warrantless write-tapping power. This case arose in the context of foreign intelligence and national security. The purpose of the FISA Amendment Act of 2008 (FAA) is to broaden the government's ability to lead electronic surveillance of communications. In that regard, the FAA's focal point is the monitoring of domestic communications between persons in foreign countries but some domestic communications may also be intercepted involuntarily. For that reason, Amnesty International et al. (the plaintiffs in this case) claimed that the state bypassed their Fourth Amendment rights, which makes that section unconstitutional. What makes this decision interesting lies in the fact that the Supreme Court is asked whether the plaintiffs can challenge the constitutionality of the FAA in spite of the absence of any evidence that their communications are actually being monitored and on the simple basis of a mere risk that communications in the United States may be monitored under this amendment[137].

According to Amnesty International et al., section 702 gives unmonitored powers to the government to conduct surveillance on American's communications in foreign countries in violation of Article III of the Constitution, the principle of separation of powers and plaintiffs' First and Fourth Amendment constitutional rights. Indeed, section 702 of the FAA created new procedures for authorising surveillance of non-Americans citizens, removed the necessity

---

136 D. LOWE, *o.c.*, p. 657.

137 D. LOWE, *o.c.*, p. 661; E. SIELSKI, "*Clapper v. Amnesty International*: Who has standing to challenge government surveillance?", *Duke Journal of Constitutional Law and Public Policy Sidebar*, 2013, pp. 51-52 and C. WILKA, *o.c.*, 2016, p. 469.

of individualized orders, reduced the role of the FISA Court and diminished the FISA Court previous review of an investigation. Due to those changes, plaintiffs are scared that FAA gives authorisation for the interception of their international communications. On the other hand, the Government argued that plaintiffs lack standing to question the validity of the FAA[138].

The respondents pleaded two sources of injuries for standing purposes. The first one is that there is a likelihood that this new amendment will allow the government to conduct surveillance of their international communications in the future. Secondly, they have been obliged to adopt expensive and demanding measures to protect their foreign communications due to the possibility that those communications would be subject to surveillance[139].

However, the U.S. Supreme Court dismissed the respondent's claim by stating that they do not have the right to challenge the constitutionality of FISA because their injury is purely speculative and not impending. The Court also stated that even if the respondents could establish an injury-in-fact, they would fail to demonstrate that their prejudice is related to the new section introduced in FISA because they can only suspect that section 702 authorises the surveillance of their international communications. On the other hand, it seems that the Court let the door open for cases where the plaintiffs can establish that there is a substantial risk that the harm will occur[140].

This case has had a lot of effects across America regarding data breach plaintiffs facing difficulties in the establishment of standing in data security class action claims. On the basis of *Clapper* decision, many federal courts in the U.S. have dismissed data breach claims because plaintiffs have lacked to establish that their risk of future harm is impending. However, none of the federal courts have defined what constitutes a sufficient injury to bring a case in data breach[141].

---

138 E. SIELSKI, *o.c.*, pp. 52-54; X. "Standing – Challenges to Government Surveillance – *Clapper v. Amnesty International USA*", *o.c.*, p. 300.

139 E. SIELSKI, *o.c.,* pp. 57-59; C. WILKA, *o.c.,* pp. 469-470.

140 D. LOWE, *o.c.*, p. 661; A. C. SAND, "Standing Uncertainty: An Expected-Value Standard for Fear-Based Injury in Clapper v. Amnesty International USA", *Michigan Law Review*, 2015, pp. 726-727; C. WILKA, *o.c.*, pp. 468 and 470; X. "Standing – Challenges to Government Surveillance – *Clapper v. Amnesty International USA*", *o.c.,* p. 298 and pp. 300-302.

141 C. WILKA, *o.c.,* pp. 470-471.

This decision was nevertheless heavily criticised from the U.S. human rights and lawyer groups. As stated by the American Bar Association, the U.S. President does not have any constitutional obligation to authorise surveillance. Furthermore, if the same decision would have been rendered by the European Court, there is a strong likelihood that the Court would have ruled in favour of the respondents[142].

Following *Clapper v. Amnesty International USA*, most of the federal district courts have ruled that, in order to stratify the standing requirements, an alleged future injury must at minimum be without doubt impending. Therefore, the risk of a future harm does not satisfy "*the certainly impending injury-in-fact requirement extensively discussed by the Clapper court*"[143]. In that sense, *Clapper* is seen by most district courts as a tightening of the standing requirements because, in this decision, the Supreme Court explained that an injury is hypothetical if its existence depends on a third party's decision. Furthermore, the Supreme Court in *Clapper* reiterated its reluctance to grant standing on the basis of speculation of whether "*an independent actor would take action in the future*"[144].

B. After Snowden

After Snowden's revelations, two significant cases were heard regarding the Fourth Amendment rights that had been violated by the NSA and the Federal Government[145].

1. Klayman et al. v. Obama et al.

The first significant case was decided by the District Court for the District of Columbia. The case concerned a judicial review that challenged the authorisation of intelligence collection of phone record metadata of all U.S. citizens[146]. Again, what is at stake concerns the balance between national security interests of the U.S. and the individual liberties of its citizens. In *Klayman v. Obama*, subscribers of U.S. telecommunications and Internet companies requested a preliminary injunction to prevent the U.S. government from collecting their telephone metadata because the program violated the Fourth Amendment. The NSA

---

142 D. LOWE, *o.c.*, p. 661.
143 C. WILKA, *o.c.*, pp. 480 and 482.
144 *Ibid*.., pp. 482-483.
145 D. LOWE, *o.c.*, p. 661.
146 G. CHAN, "Klayman v. Obama 957 F. Supp. 2d1 (D.D.C. 2013)", *Intellectual Property Law Bulletin*, 2015, p. 204; D. LOWE, *o.c.*, p. 661.

telephony metadata program implies the creation and maintenance of a historical database that will contain five years' worth of data[147].

According to the plaintiffs, "*the Government's phone metadata collection and querying program exceeds the statutory authority granted by FISA's 'tangible things' provision, 50 U.S.C. § 1861, and thereby violates the Administrative Procedure Act*"[148].

Judge Leon held that the plaintiffs could not challenge the U.S. government's compliance with federal law. Therefore, he ruled for the plaintiffs on the constitutional issue and decided that the plaintiffs showed that the telephone metadata program violated the Fourth Amendment[149]. To make his decision, Judge Leon compared the case to *Clapper* and stated that while in *Clapper* the applicants could only hypothesise that they were "surveilled", in *Klayman* there was strong evidence that the phone record metadata had been collected and that the NSA would continue to inadequately use those metadata for collection and analysis[150]. For those reasons, the U.S. District Court for the District of Columbia rightly held that "*the NSA's metadata collection program is 'indiscriminate' and 'an arbitrary invasion' amounting to a violation of the Fourth Amendment's protection against unreasonable searches and seizures*"[151].

After the Court found that a violation of the individuals' reasonable expectation of privacy to have occurred, it properly assessed the balance between individual privacy expectations and the efforts of the government to fight terrorism and came to the conclusion that such a metadata collection and analysis is unreasonable[152].

Although Judge Leon admits that "*what metadata is has not changed over time*", he concludes that in the light of the increased "*quantity of information that is now available and, more importantly, what that information can tell the Government about people's lives*",

---

147 D. P. FIDLER, *The Snowden Reader*, Bloogmington, Indiana University Press, 2015, pp. 220, 223 and 227.
148 *Klayman v. Obama*, 957 F. Supp. 2d I, IO (D.D.C. 2013), §§ 19-20.
149 G. CHAN, *o.c.,* p. 205; D. P. FIDLER, *o.c.,* p. 220; M. RAPISARDA, *o.c.*, p. 143; J. M. MASTRACCI, *o.c.*, pp. 369 and 371.
150 G. CHAN, *o.c.,* p. 205; D. LOWE, *o.c.*, pp. 661-662.
151 J. M. MASTRACCI, *o.c.*, p. 366.
152 *Ibid*., pp. 369-370.

it is "*significantly likely*" that the NSA program constitutes a breach of the Fourth Amendment[153].

Furthermore, the Court rightly found that the plaintiffs would suffer an irreparable harm if their request for relief was not granted. It also stated that although the prevention of terrorism constitutes a justification for the collection and retention of the data, the Court found that telephone metadata collection and analysis is a great issue that considerably affects the public interest[154].

To sum up, by this decision the Court correctly affirms the supremacy of the privacy expectation over the nature and immediacy of domestic terrorism concerns[155]. This decision is in line with what this research has acknowledged[156].

This decision and Judge Leon's reasoning were received positively by NSA critics, Snowden and his supporters[157]. On the other hand, some authors such as J. M. Mastracci, have expressed their reservations on Judge Leon's approach. Indeed, Judge Leon recognises the highest importance of identifying unknown terrorist operatives and preventing terrorist attacks[158] but, according to him, the government's primary interest "*is not merely to investigate potential terrorists, but rather, to do so faster than other investigative methods might allow*"[159]. However, for J. M. Mastracci, the government's central interest is rather to prevent domestic terror attacks that they might otherwise not be able to prevent without their investigation tool. Furthermore, this author considers that though Judge Leon expressed his "*serious doubts about the efficacy of the metadata collection program as a means of conducting time*" due to "*the utter lack of evidence that a terrorist attack has ever been prevented [thanks to] the NSA database*", characterizing the program as ineffective because of the unsettling nature of immediate modern domestic terrorism threats would go too far[160].

---

153 *Klayman v. Obama*, *o.c.,* §§ 35-37.
154 G. CHAN, *o.c.,* p. 206.
155 J. M. MASTRACCI, *o.c.*, pp. 373-374.
156 N.B.: The U.S. government appealed the decision and the U.S. Court of Appeal rendered its judgment in August 2015.
157 D. P. FIDLER, *o.c.,* pp. 220-221.
158 J. M. MASTRACCI, *o.c.*, p. 373.
159 *Klayman v. Obama*, *o.c.,* §§ 39-40.
160 J. M. MASTRACCI, *o.c.*, p. 373.

2. American Civil Liberties Union et al. v. James R. Clapper et al.

Eleven days after the *Klayman v. Obama* decision, Judge Pauley III of the U.S. District Court of Southern district of New York took an opposite view in its judgement, rejecting the plaintiffs' preliminary injunction. Like Judge Leon, he held that the federal law does not permit to say that Section 215 of the USA PATRIOT Act did not support the telephone metadata program. However, Judge Pauley considered that the claim would fail on the merits and examined how Section 215 entitles the telephone metadata program. According to him, the program did not violate the First or Fourth Amendments. Indeed, in this judgement Judge Pauley refers to a number of NSA investigations where he considers that the NSA's surveillance through bulk telephony metadata is justified. He therefore considers that those orders are lawful, even if he correctly recognises that if left unchecked this investigative tool can jeopardize individuals' liberty. In the case at hand, he estimates that there was no evidence that the U.S. Government had used any of the bulk telephony data to another purpose than bypassing terrorist attacks[161].

In this case, the plaintiffs requested a declaratory judgment that would (1) declare that the program exceeded the statutory authority provided by Section 215 of the USA PATRIOT Act and, (2) state that the program constitutes a violation of the First and Fourth Amendments of the U.S. Constitution. Additionally, they asked for a permanent injunction that would forbid the government to continue the collection of their telephony metadata. Judge Pauley nevertheless rejected those claims and stated in favour of the government[162].

Regarding the Fourth Amendment, according to the American Civil Liberties Union (ACLU), the analysis of bulk telephony metadata has significant drawbacks since it can reveal a lot of personal information about a person such as his religion, political associations, support for particular political causes etc. But, on the other side, the Government does not know to who the telephone numbers belong to. Another argument of ACLU is that there are other ways for the government to achieve its objective without having to first build its own database of every American's call records. In general terms, the ACLU's pleading shows a fundamental misunderstanding of what ownership of telephony metadata is[163].

---

161 D. P. FIDLER, *o.c.,* p. 228; D. LOWE, *o.c.*, p. 662; M. RAPISARDA, *o.c.,* p. 141.
162 E. E. CONNARE, *o.c.,* p. 397.
163 D. P. FIDLER, *o.c.,* pp. 233-235.

As regard to the First Amendment, the ACLU alleges that "*[t]he fact that the government is collecting this information is likely to have a chilling effect on people who would otherwise contact Plaintiffs*"[164]. The government responded that "*surveillance consistent with Fourth Amendment protection […] does not violate First Amendment rights, even though it may be directed at communicative or associative activities*"[165]. For his part, Judge Pauley conceded the government's argumentation. Therefore, it is unnecessary to decide whether or not the First Amendment has been violated in the absence of a Fourth Amendment violation because the bulk metadata collection does not seriously affect the First Amendment rights[166].

To sum up, in this case Judge Pauley acknowledged that it is well established and recognized by the American courts that the right to data privacy is a fundamental right. However, and has previously highlighted, this right is not absolute. Concerning an eventual breach, there is no evidence that the bulk telephony metadata collected by the government have been used for any other purpose than investigating and preventing terrorist attacks. Furthermore, the bulk telephony metadata collection program is subject to executive and congressional oversight and, even if there have been unintentional violations of guidelines, those were the result of human error and of complex computer programs that support this tool[167]. For those reasons, the NSA's bulk telephony metadata collection program is lawful[168].

The different conclusions reached by Judge Leon in *Klayman v. Obama* and Judge Pauley in *ACLU v. Clapper* illustrates the divisions in the American body politic following Snowden's revelations[169].

It has to be noted nevertheless that, after *Klayman v. Obama* and *ACLU v. Clapper*, all branches of U.S. government have reconsidered the legality, effectiveness and morality of data mining and data collection by national security agencies. Thus, the Congress took

---

164 *American Civil Liberties Union et al. v. James R. Clapper et al*., 959 F. Supp. 2d 724, 731 (S.D.N.Y.2013), § 35.

165 Memorandum & Order at 45, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013).

166 D. P. FIDLER, *o.c.,* p. 235.

167 *Ibid*., pp. 237-238.

168 N.B.: The plaintiffs appealed against this decision. The appellate court heard oral arguments in early September 2014 and a decision was rendered in October 2015.

169 D. P. FIDLER, pp. 228-229.

measures to reform the relevant legislation and the executive power made suggestions to restrict overreaching by the intelligence agencies[170].

These cases are relevant as they illustrate how the U.S. Courts have chosen to deal with the issue of privacy in the counterterrorism context. In that regard, in *Clapper* the U.S. Supreme Court argued that the injury of the respondents is purely speculative and not impeding. However, after Snowden's revelations, Judge Leon relied on *Clapper* to rightly recognise that surveillance programs of the NSA violate the Fourth Amendment in *Klayman v. Obama*. Unfortunately, not all courts followed this reasoning. Thus, Judge Pauley took the side of the governments by saying that there is no evidence that the data collected has been used for other purposes than counterterrorism. In the light of the above, it seems that even though there is no evidence of the use of the information in another context than counterterrorism, there is still a risk that this information will be used for other purposes. Furthermore, as already mentioned, governments tend to give to the word "terrorism" a very extensive definition and, therefore, could justify their violations to privacy in the name of the fight against terrorism in circumstances that do no fall under most people's perception of terrorism. This could lead to dangerous abuses. Moreover, this research showed that the misuse of this information is only one among many risks caused by data mining. The justification of Judge Pauley looks therefore inadequate. However, as explained above, the right to security and the right to privacy cannot be equally protected at the same time and one of them will inevitably prevail over the other. The answer to the question to know which one will prevail will vary among the importance that one grants to each right. Let us recall nevertheless that the infringement of one human right to protect another is only justified if it's necessary and proportionate. This is a case-by-case analysis that has to be made every time the question of the violation of one of those rights is raised. That being said, this research has assessed that surveillance programs put an important strain on the right to privacy. Although it might be necessary to protect national security, it is certainly not proportionate.

---

170 F. FABBRINI, *o.c.,* p. 9.

Conclusion

The increase of the evolution in technologies has not only created a new mean for terrorists to spread their ideology, but has also provided a new tool for governments to fight terrorism. This has led to the creation of national databases that collect, analyse and store personal data and information on individuals on a very large scale. Those measures have been justified by the increase of the security but the fact remains that this "dataveillance" has considerably reduced the protection of other human rights, especially the right to privacy. The proportionality of Internet surveillance affects the fundamental values of a democratic society and raises serious constitutional questions in many states. Nevertheless, in response to the terrorist threat, states feel obliged to take the most drastic actions, even if it consists of infringing their usual human rights obligations that are applicable in "ordinary" times. However, as we know, warfare has evolved and terrorism is not a passing phenomenon and there is no end in the fight against terrorism[171].

Therefore, we observe a constant tension between the right to security and, on the other and, the right to security. This tension is increased by the international cooperation that leads to data sharing and that allows governments to bypass constitutional standards on privacy. In addition, these measures are, most of the time, adopted on an emergency basis and are meant to be temporary but, once introduced, become permanent and are even extended into the general law[172]. We observe that the more broadly drafted a legislation is, the wider the powers of counterterrorism agency officers are and the deeper they can therefore intrude into the everyday lives of citizens. Therefore, a broad group of citizens fall into their intelligence systems. According to D. Lowe, national security and individual liberty are two inclusive interests. Indeed, although individual liberty is a fundamental right that must be protected from unnecessary state incursion by the judiciary, at the same time protecting citizens from terrorist attacks is equally important. Both governments and their terrorism agencies must nevertheless assess the dangers such measures confer to individuals' liberties and balance those measures with regard to the proportionality principle[173]. Hence the question arises to know whether the counterterrorism measures are a threat to the right to data protection.

---

171 I. BROWN and D. KORFF, *o.c.,* p. 120.
172 *Ibid*., p. 131.
173 D. LOWE, *o.c.*, pp. 668-669.

In order to answer that question, this research has shown how data mining relies on the idea that if terrorists plan an attack, they will engage into transactions that will produce data. Furthermore, an algorithm is used to identify targets and direct the police and authorities' attention on them. Indeed, the idea behind counterterrorism measures is to identify individuals that might commit terrorist crimes and prevent the occurrence of such attacks. However, although that data mining is a powerful tool in that context, it goes hand in hand with many risks and drawbacks such as the fact that some individuals can be wrongfully targeted, that it may provide erroneous or incomplete information, that it can be misused by authorities, that this data is collected without the consent or notification of the individuals concerned, that it provides a mean for the state to intrude in individuals' private life, etc.

Furthermore, the instruments put in place in order to prevent terrorist activities have led the police to target not just criminal but also more generally deviant behaviour. In the context of the fight against terrorism, it means that individuals are targeted because they are suspected of being terrorists or to be opposed to the constitutional legal order, even before they commit any criminal offence. Those targets are identified through profiling, which is based on algorithms that are effectively unchallengeable and lead to the targeting of innocent people that are wrongly identified as suspected terrorists. Moreover, we observe that minority groups are more likely to be targeted by these measures, which generates discrimination[174].

Although data mining and profiling certainly contribute to prevent terrorism, there is still a high proportion of real terrorists that are not identified as such. The question of the efficiency of those programs then arises. In that regard, this research observed that we are given up freedom without gaining security. Furthermore, those measures are accompanied by several drawbacks like the fact that all of us are placed under a general and precautionary mass surveillance that collect a significant part of our activities. The massive data collection and profiling that we are facing is threatening the most fundamental values of the democratic society at both national and international level[175].

In sum, data mining and profiling allow the state to have an extremely close control over its citizens' lives on a very large scale. Regarding the small amount of terrorists among us, these measures do not seem to be proportionate. Therefore, some argue in favour of a relaxation or

---

174 I. BROWN and D. KORFF, *o.c.*, p. 131.
175 *Ibid*., pp. 131-132.

a reduction of constitutional standards but this research argues that it is precisely because there is a lot at stake that governments should be cautious and, consequently, that data mining should be subjected to meticulous procedures.

As this research has demonstrated, the right to data privacy is a fundamental right but it is not absolute. States are now dealing with the difficult task to balance competing human rights interests. Indeed, they must protect their nationals against terrorist treats and, at the same time, they must safeguard individuals' fundamental rights, including persons suspected or convicted of terrorist activities[176]. Some human rights can be restricted in their application when they are objectively justified by the circumstances and if it's necessary and proportionate. To know whether or not the security may override privacy will depend on the approach taken. In that regard, the EU has a wider vision of the right to privacy than the U.S. and those two different approaches reflects the complexity of the problem. It has been argued that these differences lead to insecurity and that it is urgent that the international community adopts a binding document on the issue.

Nevertheless, the international community has not set aside this question. Indeed, different instruments have been adopted in order to resolve the issue and the most important is probably the UNGA resolution on "The Right to Privacy in the Digital Age". Notwithstanding its neutral tone, it has the benefit to aim attention to the intrusive mass surveillance we face due to the Internet and digital media environment. Another important document is the report of the OHCHR that gives a broad understanding of what constitutes an interference with privacy. Based upon this fragmentation at the international level, this research has argued that there is a need to develop and amend the existing rules, but also jurisprudence of international human rights courts and bodies in order to create a binding international instrument. Furthermore, there is a need to go beyond a general right to data protection and to provide more particular rights to individuals. Also, certain domestic and regional approaches can be useful to offer a better protection of the individuals in the digital age[177].

In the end, many authors rightly pled in favour of an update in privacy protections in order to face the technological developments. Yet, the question to know how to achieve this result

---

176 *Ibid*., p. 131.
177 K. LACHMAYER, *o.c.,* p. 101.

remains[178]. This research demonstrated that the adoption of a more sophisticated concept of data privacy is necessary in a world where digital technologies are more and more prominent and used, especially in the fight against terrorism. In order to challenge and limit transnational surveillance measures and data sharing between states, this research has shown that a right-based approach is necessary. Efforts at the domestic level are not irrelevant but transnational cooperation and international agreements are also necessary to address these issues. In that regard, the international human rights regimes offer certain protection of privacy but a more differentiated approach is needed in order to deal and address all the various aspects of data privacy in the context of international surveillance. An international framework on data privacy, focusing on questions of state surveillance, seems to be a suitable answer to international cooperation of intelligence and law enforcement agencies[179].

However, the question remains: how to prevent serious crime and terrorism without impeding on fundamental rights at the same time[180]?

The complexity of the answer to this question has been demonstrated through the U.S. Court's approaches. Indeed, three important cases have been analysed and reflect the different interpretations that can be adopted depending on whether the judge is rather a proponent of privacy or of security.

To conclude, the question to know whether or not counterterrorism threatens the right to data protection is a more complicated one than it would appear. There is no easy answer as it will depend on the perspective taken: either proponents of privacy, either proponents of security. Both rights can obviously not be simultaneously respected. Therefore, it will depend on whether one considers the right to privacy more important than the right to security or not. This research has recognised the importance of security but argued that measures such as data mining and profiling are not efficient enough and are not proportionate enough to deal with the terrorist threat. Furthermore, the justifications given by governments and courts are not adequate. Indeed, the safeguards to protect privacy are not sufficient. A proof of that is the many cases brought in front of domestic jurisdiction regarding that matter. Therefore, new international instruments should be developed.

---

178 F. FABBRINI, *o.c.,* p. 13.
179 K. LACHMAYER, *o.c.,* 102.
180 A. VEDASCHI A. and V. LUBELLO, *o.c.,* p. 14.

Bibliography

Legislation

U.S. legislation

U.S. Code.

U.S. Constitution Amendment IV.

Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 501(a)(1), 115 Stat. 287 (2001).

USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 (2001).

International legislation

Universal Declaration of Human Rights.

International Covenant on Civil and Political Rights.

European Convention on Human Rights.

The Right to Privacy in the Digital Age, GA Res 68/167, UN GAOR, 3rd Comm, 68th sess, 70th plen mtg, Agenda Item 69(b), UN Doc A/RES/68/167 (21 January 2014, adopted 18 December 2013.

Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the OHCHR*, U.N. Doc. A/HRC/27/37, 30th June 2014.

Cases

United States v. Brigoni-Ponce, 422 U.S. 873, 885-887 (1975).

Whren v. United States, 517 U.S. 806, 813 (1996).

Clapper v. Amnesty International USA, 568 U.S., 11-1025 (2013).

Klayman v. Obama, 957 F. Supp. 2d I, IO (D.D.C. 2013).

American Civil Liberties Union et al. v. James R. Clapper et al., 959 F. Supp. 2d 724, 731 (S.D.N.Y.2013).

Memorandum & Order at 45, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013).

Literature

Books and legal articles

BAYRAMZADEH K., "Les Etats faillis et le terrorisme transnational", *Rev. Dr. Ulg*, 2015, pp. 99-121.

BROWN I. and KORFF D., "Terrorism and the Proportionality of Internet Surveillance", *European Journal of Criminology*, 2009, pp. 119-134.

CHAN G., "Klayman v. Obama 957 F. Supp. 2d1 (D.D.C. 2013)", *Intellectual Property Law Bulletin*, 2015, pp. 203-206.

CONNARE E., "*ACLU v. Clapper*: The Fourth Amendment in the Digital Age", *Buffalo Law Review*, 2015, pp. 395-419.

CURRAT P., "Le droit face à de nouvelles générations de guerre et de terrorisme", *Revue de l'avocat*, 2016, pp. 103-113.

DREHER A., GASSEBNER M. and SIEMERS L.-H., "Does terrorism threaten human rights? Evidence from panel data", *The Journal of Law and Economics*, 2010, pp. 65-93.

FABBRINI F., "Privacy and national security in the digital age – European and comparative constitutional perspectives", *Tilburg Law Review*, 2015, pp. 5-13.

FAYYAD U., PIATETSKY-SHAPIRO G., SMYTH P., "From Data Mining to Knowledge Discovery in Databases", *Al Magazine*, 1996.

FENWICK H., "Proactive counter-terrorist strategies in conflict with human rights", *International Review of Law Computers and Technology*, 2008, pp. 259-270.

FIDLER D. P., *The Snowden Reader*, Bloogmington, Indiana University Press, 2015.

GEARTY C., *Liberty & Security,* Cambridge, Cambridge: Polity Press, 2012.

JOHNS F., "The deluge", *London Review of International Law*, 2013, pp. 9-34.

JOYCE D., "Privacy in the digital era: human rights online?", *Melbourne Journal of International Law*, 2015, pp. 1-16.

LACHMAYER K., "Rethinking privacy beyond borders – Developing transnational rights on data privacy", *Tilburg Law Review*, 2015, pp. 78-102.

LOWE D., "Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty", *Terrorism and Political Violence*, 2016, pp. 653-673.

MASTRACCI J. M., "*Klayman v. Obama*: The D.C. District Court misinterprets the NSA metadata collection program as a violation of individual Fourth Amendment rights", *Tulane Journal of Technology and Intellectual Property*, 2014, pp. 365-374.

MILANOVIC M., "Human rights treaties and foreign surveillance: privacy in the digital age", *Harvard International Law Journal*, 2015, pp. 81-146.

RAPISARDA M., "Privacy, technology, and surveillance: NSA bulk collection and the end of the *Smith v. Maryland* era", *Gonzaga Law Review*, 2015/16, pp. 121-158.

RENKE W. N., "Who controls the past now controls the future: counter-terrorism, data mining and privacy", *Alberta Law Review*, 2006, pp. 779-823.

ROSEN J., "The naked crowd: Balancing privacy and security in an age of terror", *Arizona Law Review*, 2004, pp. 607-619.

ROSENZWEIG P., "Privacy and counter-terrorism: the pervasiveness of data", *Case Western Reserve Journal of International Law*, Vol. 42, Issue 3 (2010), pp. 625-646.

SAND A. C., "Standing Uncertainty: An Expected-Value Standard for Fear-Based Injury in Clapper v. Amnesty International USA", *Michigan Law Review*, 2015, pp. 710-738.

SIELSKI E., "*Clapper v. Amnesty International*: Who has standing to challenge government surveillance?", *Duke Journal of Constitutional Law and Public Policy Sidebar*, 2013, pp. 51-69.

VEDASCHI A. and LUBELLO V., "Data retention and its implications for the fundamental right to privacy", *Tilburg Law Review*, 2015, pp. 14-34.

WILKA C., "The effects of *Clapper v. Amnesty International USA*: An improper tightening of the requirement for article III standing in medical data breach litigation", *Creighton Law Review*, 2016, pp. 467-492.

X. "Standing – Challenges to Government Surveillance – *Clapper v. Amnesty International USA*", *Harvard Law Review*, 2013, pp. 298-307.

Press articles

GREENWALD G., "NSA Collecting Phone Records of Millions of Verizon Customers Daily", *The Guardian*, June 6, 2013, available at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (accessed on March, 30th 2017).

WATT N., "PRISM Scandal: European Commission to Seek Privacy Guarantees from U.S.", *The Guardian*, June 10, 2013, http://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees (accessed on March, 30th 2017).

Others

OBAMA B., President of the United States, Remarks by the President on Review of Signals Intelligence, 17th January 2014, available at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence (consulted on 6th June 2017).

Report of the Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* (Washington, D.C., March 2004), online: Center for Democracy and Technology, https://www.cdt.org/files/security/usapatriot/20040300tapac.pdf (consulted on 1st June 2017).

U.N. Human Rights Comm., Concluding Observations on the Fourth Report of the United States of America, advance unedited version, March 2014, p. 9, available at http://justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf (consulted on 8th June 2017).

Office of the High Commissioner for Human Rights, Special rapporteur on the right to privacy, available at http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx (consulted on 8th June 2017).

The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World", 12 December 2013**,** available at https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (consulted on 6th June 2017).