A GLOBAL PERSPECTIVE ON THE PROTECTION OF PRIVACY AND RELATED HUMAN RIGHTS IN COUNTERING THE USE OF INTERNET FOR TERRORIST PURPOSES

by

CRISTINA SISERMAN*

The present study provides a "global" perspective on the protection of privacy in the fight against the use of Internet for terrorist purposes. The paper reiterates the fact that in countering terrorism, the right to privacy is often challenged by the right to security. Its main objective is twofold: firstly, to put forward the importance that the right to privacy represents for all democratic societies obeying the rule of law and, secondly, to show that security is an important right that has also been lately challenged due to the advancements in technology, which have been abused for terrorist purposes. The paper advocates for the implementation of a coherent international framework, with clear and efficient norms, which would enable States to apply equal standards in the investigation of Internet-related matters and which would ensure the respect of privacy and correlated human rights, while providing an efficient setting for cooperation between States and organisations.

KEYWORDS:
privacy, security, terrorism, Internet, human rights, international cooperation, harmonised legislation

1. INTRODUCTION

In 2009, Said Namouh, a Moroccan citizenship residing in Canada, was convicted of four terrorism-related charges for plotting attacks in Germany and

* cristinasiserman@gmail.com; Cristina SISERMAN is currently a Phd Student in International Law at the University of Vienna, Austria. She has worked as a trainee at the United Nations Office on Drugs and Crime (UNODC) and the Preparatory Commission for the Comprehensive Nuclear Test-Ban Treaty Organization (CTBTO) in Vienna, Austria.

Austria in order to get the NATO nations to withdraw troops from Afghanistan[1]. In March 2007, the defendant, posted a video, demanding the governments of Austria and Germany to "withdraw their troops from peace-support missions in Afghanistan or else face grave consequences"[2]. Following the broadcast of the video, the Austrian authorities initiated an investigation that included wire-taps on various online communications between Said Namouh and Mohammed Mahmoud, an Austrian national living in Vienna, Austria[3].

The communications among the two defendants, conducted in Arabic, consisted of Voice over IP and Internet chat sessions. The communications disclosed issues associated with jihad and plans for a terrorist attack in Europe. The investigations conducted by both Austrian and Canadian authorities revealed that Mr. Namouh was spending considerable time on the Internet in order to be in constant contact with jihadists around the world, including the Global Islamic Media Front, which disseminates propaganda and provides jihadists with tools (bomb manuals, encryption software etc.) needed to carry out jihad[4].

Between 3 June and 9 September 2007, Mr Namouh (Canada) and Mohammed Mahmoud (Austria) had around 31 online conversations about carrying out a bombing at an undisclosed location in Europe, on manufacturing of weapons like explosive belts, financing issues and travel plans to meet other persons in Maghreb and Egypt for final preparations[5].

On 12 September 2007, the Austrian and Canadian authorities carried out simultaneous arrests of Namouh and Mahmoud[6]. During the trial, Namouh's defence challenged several aspects of the prosecution, which included constitutional arguments based on the freedom of expression and right to privacy in communication[7]. Despite the invoked arguments,

---

1 Global Jihad, 2009, Said Namouh convicted in Canada. Available online: http://www.globaljihad.net/view_news.asp?id=1102 (last accessed 05.08.2012).

2 Mantel, B., 2009, Terrorism and Internet, CQ Global Researcher, No. 3, p. 285-310. Available online: http://library.cqpress.com/globalresearcher/ (last accessed 05.08.2012).

3 United Nations Office on Drugs on Crime, 2012, The Use of Internet for Terrorist Purposes, Vienna, p. 84-86.

4 National Coordinator for Counterterrorism, 2010, Jihadists and the Internet, Hague, Netherlands, p. 44. Available online: http://www.fas.org/irp/world/netherlands/jihadists.pdf (last accessed 05.07.2012).

5 United Nations Office on Drugs and Crime, cited supra note 3, p. 85.

6 Ibid., p. 84-86.

7 Ibid., p. 85.

Namouh was sentenced[8] under the Canadian Anti-Terrorism Act[9] to life in prison in Canada for distributing terrorist propaganda online[10].

The case of Said Namouh is just one of the many legal cases[11]involving the use of Internet for terrorist purposes and showing the real dangers that these activities represent. In a recent publication of the United Nations Office on Drugs and Crime, Terrorism Prevention Branch, the experts provided a relevant collection of cases[12] on how defendants used the Internet and related technology for terrorist purposes. These cases brought forward wide discussions regarding the importance of special investigative techniques in finding terrorism-related content on the Internet, as well as on the rights that suspects have during the investigation and prosecution. They have also generated considerable debate among lawyers and specialists on the topic of protection of privacy and correlated human rights while countering terrorism. The main issue that has been raised, was how could the right to privacy be balanced in regard to the right to security, i.e. to what

[8] In rendering the sentence the Court of Quebec stated: "The Court has no doubt on this subject. The context of these messages clearly refers to real actions encouraged by the GIMF. Death and destruction are everywhere. The jihad promoted by the GIMF is a violent one. This promotion clearly constitutes counselling ('encouragement') and sometimes a threat of terrorist activity. Therefore, this activity clearly falls within the definition of terrorist activity within the meaning of Section 83.01 Criminal Code". For the whole judgement See: R c. Namouh, 2009. Available online: https://www.unodc.org/tldb/pdf/Canada/Jurisprudence/Unconsitutionality_Claim_2009_FR.pdf (last accessed 05.07.2012).

[9] The Canadian Anti-Terrorism Act was passed by the Liberal government of Canada on December 18, 2001. The Act has been widely criticised for the expanded powers that was granting, such secret trials, preemptive detention and surveillance powers. It has also been considered as being incompatible with the Canadian Charter of Rights and Freedoms, especially in what was concerned the right to privacy. For more information *See* BC Freedom of Information and Privacy Association, 2005, Canada's Anti-terrorism Act: an unjustified limitation of freedom of information and privacy rights, The Law Foundation of British Columbia, p. 1-22.

[10] Leuprecht, C., 2011, Cross-border Leuprecht, C., 2011, Cross-border terror networks: creating markets of opportunity?, p. 18. Article available online: http://www.erdr.org/textes/leuprecht_hataley.pdf (last accessed 05.08.2012).

[11] Other controversial cases that raised issues regarding the use of Internet for terrorist purposes and question relating to privacy and freedom of expression in the last years are: Sami Al-Hussayen who was accused of designing, creating and maintaining web sites that support terrorism, but who was in the end acquitted by the appeals court on the ground that the suspects must have a clear intent to engage in terrorism; Younis Tsouli who has been accused of supporting and conducting propaganda for jihad on the Internet and who was found guilty by the German court on the basis that his postings went beyond expressing sympathy for terrorist groups and extended to recruiting. For detailed information on these cases See Mantel, B., Ibid.

[12] Some of the most relevant legal cases in which Internet has been used for terrorist purposes include: R v Zafar, Butt, Iqbal, Raja and Malik, 2008. Judgement available: http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/13_02_08beaumont.pdf (last accessed 05.08.2012); R v Terence Roy Brown, 2011. Judgement available: http://www.thelawpages.com/court-cases/Terence-Roy-Brown-6475-1.law (last accessed 05.08.2012); R v. Tsouli, Mughal and Al Daour, 2007. For more on the case see: http://news.bbc.co.uk/2/hi/6268934.stm (last accessed 05.08.2012).

degree could surveillance programmes be implemented without infringing the right to privacy?

Finding an answer to the questions outlined above is impossible without first understanding what privacy entails. Privacy is a complex legal notion with many dimensions and implications. The Special Rapporteur on the promotion of human rights and fundamental freedoms while countering terrorism defined privacy as a fundamental human right which provides individuals with "an area of autonomous development, interaction and liberty"[13]. The 1948 Universal Declaration of Human Rights[14], the 1966 International Covenant on Civil and Political Rights[15], as well as the main regional human rights instruments, such as the 1950 European Convention on Human Rights[16], the 1978 American Convention on the Human Rights[17] or the 1990 Cairo Declaration on Human Rights in Islam[18] recognise privacy as an integral part of the right to respect for private life, which was consecrated as a human right, part of the group of civil and political rights. Article 8 of the European Convention on Human Rights guarantees the right to private life

[13] Humans Rights Council, 2009, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development – Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, p. 5. Available online: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf (last accessed, 05.08.2012).

[14] Art. 21 of the Universal Declaration of Human Rights provides that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[15] Art. 17 of the International Covenant on Civil and Political Rights provides that "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; 2. Everyone has the right to the protection of the law against such interference or attacks." Art. 4 of the Covenant allows States to derogate from art. 14 only in case of a state emergency threatening the life of the nation, but they are subject to conditions.

[16] Art. 8 of the European Convention on Human Rights stipulates in its paragraph 1 "Everyone has the right to respect for his private and family life, his home and his correspondence." Paragraph 2 stipulates that "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[17] Art. 11 of the American Convention on the Human Rights provides in its three paragraphs that "1. Everyone has the right to have his honour respected and his dignity recognized.; 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation.; 3. Everyone has the right to the protection of the law against such interference or attacks."

[18] Art. 18 of the Cairo declaration of the Human Rights in Islam provides that "(a) Everyone shall have the right to live in security for himself, his religion, his dependants, his honour and his property; (b) Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference."

that encompasses the special right, which in European countries is usually referred to as "data protection" and in the United States of America as "privacy". Despite the different terminological uses, these international instruments aim to regulate the gathering, processing and storing of data in order to safeguard privacy and related interests of the persons in cause[19]. The Special Rapporteur notes that privacy is not always mentioned as a separate right in the constitutions[20]. However, nearly all States recognize its value as a matter of constitutional significance. In the Special Rapporteur's view, "in some countries, the right to privacy emerges by extension of the common law of breach of confidence, the right to liberty, freedom of expression or due process. In other countries, the right to privacy emerges as a religious value"[21]. In this light, it appears that "privacy is not only a fundamental human right, but also a human right that supports other rights and it forms the basis of any democratic society"[22].

Despite the urgent need of finding efficient means to counter terrorism, many States and international organisations, among which the United Nations through its Commissioner for Human Rights and the European Union, have pointed out the danger represented by the potential violations of privacy (data gathering) and other human rights. Many violations occur as a consequence of processing vast amount of sensitive personal data, ethnic profiling and creation of privacy-intrusive databases[23]. However, no activity, even one as important as countering terrorism, should unconditionally override respecting of privacy and related human rights. These have to be respected in all phases of counter-terrorism initiatives, from preventing intelligence gathering to ensuring due process in the prosecution of suspects. States have a duty to make sure that any restriction on privacy rights is necessary, proportionate and adequately regulated[24].

---

[19] Bygrave, L., 2010, Privacy and data protection in an international perspective, Stockholm Institute for Scandinavian Law, p.1. Available online: http://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Privacy%20and%20Data%20Protection%20in%20International%20Perspective.pdf (last accessed 05.08.2012).

[20] Humans Rights Council, 2009, Ibid., cited supra note 13, p. 7.

[21] Ibid., p. 7.

[22] Ibid., p. 7.

[23] United Nations Human Rights, 2010, Office of the High Commissioner for Human Rights, Safeguard privacy while countering terrorism. Available online: http://www.ohchr.org/EN/NewsEvents/Pages/CounterTerrorismAndPrivacy.aspx (last accessed 05.08.2012).

[24] Ibid.

The main objective of the present study is to discuss the limits between the right to privacy and the States' obligation to undertake preventive and sustained measures in order to counter illegal acts in the context of the use of the Internet for terrorist purposes. States need to avert the destructive impact of terrorism on human rights (such as the right to liberty and physical integrity of the individuals) and in the same time to ensure the territorial integrity and security of States[25]. Since the protection of human rights is a core value of almost all international legal systems, the principles of human rights and fundamental freedoms, as they appear in the international instruments presented above, need to be respected at all times.

In the first part, the study provides a short introduction on the global and regional strategies in countering the use of Internet for terrorist purposes and discusses the way "privacy" is framed within the universal and regional legal instruments. In the second part, the study addresses the issues of surveillance and data profiling for counter-terrorism purposes and it identifies different ways privacy can be violated while conducting these activities. The study further presents some of the existing clashes between the right to privacy and the increasing surveillance methods. Since their laws are very varied, States encounter difficulties in adopting a uniform legislation for international cooperation in the field of data collection and surveillance measures. In this line of thought, by calling on the urgent need to adopt clear standards and harmonised legislation, the third part of the study aims to show some of the possible ways in which the right to privacy, on one side, and right to security, on the other side, can coexist while countering terrorism. In the end, the study recalls the global dimension that both terrorism and Internet have and identifies some of the standards that States should adopt in order to guarantee the protection of privacy and correlated human rights in the fight against terrorism.

[25] This is an idea in the same line of thought as the guidelines provided by the United Nations High Commissioner for Human Rights and the Directorate General of Human Rights of the Council of Europe. For in depth details See: Office of the United Nations High Commissioner for Human Rights, 2008, Human Rights, Terrorism and Counter-terrorism, Fact Sheet No. 32, Geneva; Directorate General of Human Rights, Council of Europe, 2005, Human rights and the fight against terrorism: The Council of Europe Guidelines, Council of Europe Publishing.

2. GLOBAL AND REGIONAL STRATEGIES IN COUNTERING THE USE OF INTERNET FOR TERRORIST PURPOSES

The applicable international legal framework related to counter-terrorism and Internet is contained in a wide range of sources, from resolutions of the Security Council, to treaties and conventions adopted at regional level and national legislation. The following section presents some of the most relevant instruments used in countering the use of Internet for terrorism purposes and discusses the way these instruments interact with privacy.

2.1 UNIVERSAL LEGAL INSTRUMENTS AND REGULATIONS

Terrorist use of Internet is a transnational problem, requiring an integrated response, across borders and national criminal justice systems. At international level, the universal counter-terrorism legal instruments[26], adopted under the auspices of the United Nations and its specialised agencies, comprise a wide range of sources (resolutions, treaties, jurisprudence and customary international law). Some of these instruments are only biding to the signatory States, which are responsible for enforcing the provisions through the domestic criminal justice system. Despite the wide coverage of universal counter-terrorism legal instruments, there is no universal convention which has been specifically adopted relating to the prevention of terrorist use of the Internet[27]. It was only in December 2010 that the general Assembly adopted the resolution 65/230[28], requesting the Commission on Crime Prevention and Criminal Justice to establish an intergovernmental expert group to conduct a comprehensive study on cybercrime and responses to it by the Member States.

---

[26] The universal legal instruments cover acts from aircraft hijacking to nuclear terrorism and they cover terrorists acts such as acts of aviation sabotage, acts of violence at the airport, acts against the safety of maritime navigation, acts against the safety of fixed platforms located on the continental shelf crimes against internationally protected persons, acts of unlawful taking and possession of nuclear material, acts of terrorist bombing, acts of funding of the commission of terrorist acts etc. For more information on the 18 universal counter-terrorism legal instruments as well as their texts in the official languages of the United Nations, See the United Nations Office on Drugs and Crime portal: https://www.unodc.org/tldb/en/universal_instruments_list__NEW.html (last accessed 05.08.2012).

[27] United Nations Office on Drugs and Crime, cited supra note 3, p. 17.

[28] General Assembly resolution 65/230 on Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 2010. Available online: http://www.unodc.org/documents/justice-and-prison-reform/AGMs/General_Assembly_resolution_65-230_E.pdf (last accessed 05.08.2012).

The Global Counter Terrorism Strategy, adopted in 2006 by the General Assembly though the resolution 60/288/2006[29] constitutes a milestone in counter-terrorism initiatives. In its preamble, the resolution shows that Member States undertook the obligation, *inter alia*, "to take urgent actions to prevent and combat terrorism in all its forms and manifestations"[30]. In its following paragraphs, the resolution contains clear reference to the Internet and provides that the States assumed the responsibility to "[...] work with the United Nations with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to: (a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; (b) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard."[31] This strategy came as a result of the Secretary-General Ban Ki-Moon's policy regarding the use of Internet and his belief according to which, "the ability to generate and move finances, to acquire weapons, to recruit and train cadres, and to communicate, particularly through the use of Internet, are all essential to terrorism"[32].

The same concern was reiterated later, in the Security Council Resolution 1963, adopted in 2010 under the title "Threats to international peace and security caused by terrorist acts". The Security Council expressed "concern at the increased use by terrorists of new information and communication technologies, in particular the Internet, for the purposes of the recruitment and incitement as well as for the financing, planning and preparation of their activities."[33] Taking this into consideration, the Security Council also highlighted the need for cooperation among Member States to prevent terrorists from exploiting technology, communications and resources[34]. Recent United

---

[29] The Global Counter-Terrorism Strategy was adopted in 2006 under the form of a resolution and an annexed Plan of Action. For more details on the UN Action to Counter Terrorism See the United Nations portal: http://www.un.org/terrorism/strategy-counter-terrorism.shtml (last accessed 05.08.2012).

[30] The Global Counter-Terrorism Strategy, 2006, See the Plan of Action.

[31] The Global Counter-Terrorism Strategy, 2006, See II. Measures to prevent and combat terrorism.

[32] Report of the Secretary-General, 2006, Uniting against terrorism: recommendations for a global counter-terrorism strategy, A/60/825, p. 8.

[33] Security Council Resolution S/RES/1963 (2010), Preamble, p. 3. Available online: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/702/23/PDF/N1070223.pdf?OpenElement (last accessed 05.08.2012).

[34] Security Council Resolution S/RES/1963 (2010), Preamble, p. 3.

Nations reports[35] have also acknowledged the importance of countering terrorist use of the Internet, as the key of a comprehensive strategy.

None of the instruments mentioned above contain particular provisions regarding the guarantee of privacy or the degree to which it can be limited while countering terrorism. Privacy is thus tackled only under the general obligation of respecting human rights. However, this does not imply that privacy provisions have been overseen. Human rights obligations[36] form an integral part of the international legal counter-terrorism framework. The States have both the obligation to prevent terrorism attacks, which have the potential to undermine human rights, and also the duty to ensure that all counter-terrorism measures respect human rights. The Global Counter-Terrorism Strategy reaffirms these obligations[37], recognizing in particular that "effective counter-terrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing"[38].

2.2 REGIONAL INSTRUMENTS AND POLICIES

In 2001, the Council of Europe elaborated the Budapest Convention on Cybercrime, which is at the moment the only multilateral, legally binding instrument addressing criminal activity conducted via the Internet[39]. The Cybercrime Convention seeks to harmonize national laws relating to cybercrime, to improve domestic procedures for detecting, investigating, and prosecuting such crimes and to provide arrangements for fast and reliable international cooperation on these matters[40]. However, the Convention has

---

35 For more details See United Nations General Assembly, 2012, 66th Session, Report of the Secretary-General on United Nations Global Counter-Terrorism Strategy: activities of the United Nations system in implementing the Strategy (A/66/762); United Nations General Assembly, 2011, 66th Session, Report of the Secretary-General on Measures to eliminate international terrorism (A/66/96).

36 The most important human rights instruments adopted under the auspices of the United Nations, and also presented in the introduction of this study, include the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR), and applicable protocols.

37 For more detailed analysis of the protection of human rights while countering terrorism See United Nations General Assembly, 2010, 14th Session, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures to ensure respect for human rights by intelligence agencies while countering terrorism.

38 The Global Counter-Terrorism Strategy, 2006, See IV. Measure to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism.

39 United Nations Office on Drugs on Crime, 2012, Ibid., cited supra note 3, p. 29.

40 See the Preamble of the Council of Europe, Convention on Cybercrime, 23 November 2001. Available at: www.coe.int/cybercrime (last accessed 05.08.2012).

a series of drawbacks, as it does not cover the entire spectrum of acts in which Internet is used for terrorist purposes. Neither terrorism nor the use of Internet for terrorist purposes are mentioned in the Convention. As a result, in the view of Foggetti, the problem that arises is the need to qualify on cyber-terrorism separately, by making a conceptual division between cybercrimes and terrorism[41]. In this way, the whole offence will be punishable on the basis of different standards, laid down by States. According to the same author, the existing measures stipulated in the Convention may be applied to the recruitment, training and public provocation to commit a terrorist offence, made through the Internet. However, they do not apply to terrorist acts undertaken and completed through the Internet[42]. The Budapest Convention, despite its substantial limitations, provides in its preamble the acknowledgement of the need to ensure a proper balance between the interest of law enforcement and respect for fundamental human rights as enshrined in different conventions, which reaffirm the "right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy"[43].

At the European Union level, there is a considerable amount of measures which have been adopted in order to fight terrorism. Among these are the Council Framework Decision of 13 June 2002 on fight against terrorism[44] and the Proposal for a Council framework decision amending the Framework Decision 2002/475/JHA on the fight against terrorism[45], which makes a reference to cyber-terrorism. In this document, the Council notes that "the Internet serves in this manner as one of the principal boosters of the processes of radicalisation and recruitment: it is used to inspire and mobilise local networks and individuals in Europe and also serves as a source of information on terrorist means and methods, thus functioning as a 'virtual training camp'. The dissemination of terrorist propaganda and terrorist ex-

[41] Foggetti, N., 2009, Cyber-terrorism and the right to privacy in the third pillar perspective, Masaryk University Journal of Law and Technology, Vol. 3, No. 3, p. 368.

[42] Ibid., p. 368.

[43] See Preamble, Convention on Cybercrime, Ibid.

[44] Council Framework Decision on the fight against terrorism, 2002. Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:164:0003:0003:EN:PDF (last accessed 05.08.2012).

[45] Proposal for a Council framework decision amending the Framework Decision 2002/475/JHA on the fight against terrorism. Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007SC1425:EN:NOT (last accessed 05.08.2012).

pertise through the Internet has therefore empowered terrorists, making the terrorist threat grow"[46]. The importance of such dissemination can only be expected to increase, taking into consideration the fast growing number of users that will make the Internet an even more vital element of the modern society[47].

According to Foggetti, in the European Union, the protection of privacy under the law remains anchored to the first pillar, while the fight against terrorism and crimes takes place in the second and third pillar[48]. In the author's view, it is difficult to balance the protection of privacy with the fight against international terrorism and to assess the impact taken by institutions in order to reach these purposes[49]. But for what matters, the effort has to be made. It is necessary to protect the international and European security, but at the same time also the individuals against the abuses of authority against fundamental rights such as privacy[50].

At the European Union level, citizens dispose of a means of control, as they can appeal to the Court of First Instance and then to the Court of Justice of the European Union in case they consider that their rights have been violated. In the last years, the European Court of Human Rights has given strong recognition to data protection principles under art. 8 of the European Convention on Human Rights, especially in the cases of Peck v. the UK[51], Amann v. Switzerland[52] and Rotaru v. Romania[53]. Yet when dealing with terrorism, it can be observed that a significant part of the current jurisprudence[54] is not in favour of the protection of fundamental rights.

---

[46] See Section 2: Definition of the problem of the Proposal for a Council framework decision amending the Framework Decision 2002/475/JHA on the fight against terrorism.

[47] See Foggetti, Ibid., cited supra note 41, p. 367.

[48] Ibid., p. 370.

[49] Ibid., p. 371.

[50] Ibid., p. 373.

[51] European Court of Human Rights, 2003, Case of Peck v. United Kingdom, Application no. 44647/98. Available online: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60898 (last accessed 05.08.2012).

[52] European Court of Human Rights, 2000, Case of Amann v. Switzerland, Application no. 27798/95. Available online: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58497 (last accessed 05.08.2012).

[53] European Court of Human Rights, 2000, Case of Rotaru v. Romania, Application no. 2834/195. Available online: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586 (last access 05.08.2012).

[54] One example is the Judgement of the European Court of 3 September 2008, C-402/05 in the case Yassin Abdullah Kadi c. Council. In the case the Court claimed that the fight against terrorism prevails on fundamental rights.

3. POSSIBLE FORMS OF PRIVACY VIOLATION IN COUNTERING TERRORISM

In countering the use of Internet for terrorist purposes, situations often arise when surveillance policies clash with privacy. The violation of privacy in these cases has as a repercussion the violation of other correlated human rights. Privacy is neglected in the permanent quest of States to increase surveillance measures in order to detect potential terrorists. Notwithstanding, looking from another facet, without countering terrorism one of the most fundamental rights – the right to security and safety – may well be breached. It appears thus, that after examining each right at a time, it can be rightfully affirmed that both of them are of utmost importance. This will support our argument in the next chapter that finding a balance between the two rights is necessary for a democratic society.

3.1 CLASH BETWEEN SURVEILLANCE POLICIES AND PRIVACY PROTECTION

State counter-terrorism measures affect numerous fundamental rights. According to human rights promoters, they include the right to life (through targeted killings), liberty interests (through arbitrary detention), racial and ethnic profiling, freedom of speech and association, as well as the right to privacy[55]. According to Culnan, privacy can only exist when the usage, release and circulation of personal information can be controlled[56]. Inversely, according to Lim, invasions of privacy occur when individuals cannot maintain a substantial degree of control over their personal information and its usage[57]. These types of invasions also arise because that the search for terrorists must take place beyond national borders, with the help of third parties, which hold extensive amounts of information on individuals[58]. As seen above and reinforced by the Human Rights Rapporteur, due to technologically advanced instruments of control, human rights standards, among

---

[55] Human Rights Advocates, Counter-terrorism and the protection of human rights, Human Rights Council: 13th Session, Agenda Item 3: Countering Terrorism, p. 6.

[56] Culnan, M., 1993, How did they get my name? An Explanatory Investigation of Consumer Attitudes Towards Secondary Information Use, MIS Quarterly, Vol. 17, No. 3, p. 341, In Chung, W., Paynter, J., 2002, Privacy Issues on the Internet, Proceedings of the 35th Hawaii International Conference on System Sciences, IEEE Computer Society, p. 1.

[57] Lim. E, 2000, Electronic Commerce and the Law, Bcom(Hons) Dissertation, MSIS, University of Auckland, In Chung, W., Paynter, J., 2002, Privacy Issues on the Internet, Proceedings of the 35th Hawaii International Conference on System Sciences, IEEE Computer Society, p. 1.

[58] Humans Rights Council, 2009, Ibid., cited supra note 13, p. 13.

which also privacy, have been tested and stretched through the use of arbitrary searches; the compilation of lists and databases; the use of profiling to identify potential suspects; the accumulation of ever larger databases to calculate the probability of suspicious activities and identify individuals for scrutiny[59].

Surveillance regimes, in the name of the protection of national security[60], have a powerful effect on privacy and other rights and they sometimes seem to clash. Why is this so? As already mentioned, privacy, in addition to constituting a right in itself, serves as a basis for other rights, without which the other rights would not be efficiently enjoyed[61]. According to the Special Rapporteur, privacy is necessary to create spaces which allow individuals and groups to be able to think and develop ideas and relationships. "Other rights such as freedom of expression, association, and movement all require privacy to be able to develop efficiently"[62]. But as the Rapporteur has pointed out, there are cases in which surveillance has resulted in miscarriages of justice, leading to failures of due process and wrongful convictions. Due to the fact that terrorists operate worldwide, the data associated with their activities can be easily mixed with data pertaining to people who are not terrorists. Therefore, in Popp's view, if the governments want access to this data, then they must also have some way to protect the privacy of those who are not involved in terrorism[63]. In other words, according to Hammarberg, the Commissioner for Human Rights at the Council of Europe, surveillance may seem to work up to a point, but it can inevitably lead to actions against very large numbers of innocent people, on a scale that is unacceptable in a democratic society[64]. In his view, attempts to identify very rare incidents or targets from a very large data set are highly likely to result

[59] See Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Human Rights Council, A/HC/13/37, p.14.

[60] Human rights can be modified or limited in the pursuit of countervailing or overriding societal objectives, such as the protection of natural security. Art. 4 para. 1 of the International Covenant on Civil and Political Rights provides that "In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin."

[61] Humans Rights Council, 2009, Ibid., cited supra note 13, p. 19.

[62] Ibid., p. 19.

[63] Popp, R., Poindexter, J., 2006, Countering Terrorism through Information and privacy Protection Technologies, IEEE Computer Society, IEEE Security&Privacy, p. 19.

in unacceptably large numbers of "false positives" (identifying innocent people as suspects) or "false negatives" (not identifying real criminals or terrorists)"[65].

Which are the areas that are most affected when trying to protect privacy, through invasive means of surveillance? The Rapporteur stressed that the right to freedom of association and assembly are often threatened by the use of surveillance[66]. He showed that expanded surveillance powers sometimes lead to "function creep". This happens when police or intelligence agencies label other groups as terrorists in order to allow the use of surveillance powers which were given only for the fight against terrorism[67] [68]. Moreover, there are also concerns regarding the freedom of movement, which can also be affected by surveillance and data policy[69]. In these cases, according to the Rapporteur, "the creation of secret watch lists, excessive data collection, sharing and imposition of intrusive scanning devices or biometrics, all create barriers to mobility"[70]. There is an increasing collection of data, especially at the EU level, about people travelling internationally. This information is shared among different intelligence networks and profiles and watch lists are developed.

Despite the existing legislative clash between surveillance policies and privacy, a lot of governments still find surveillance and data profiling as one of the most efficient tools in countering terrorism. Might it this be due to the fact that each presupposes each other?[71] In other words, what if the right to privacy depends upon the existence of surveillance and vice versa? Could it be the reason why surveillance is such a powerful tool? These are some of the questions that are targeted in the following section.

---

[64] Hammarberg, T., 2008, Protecting the right to privacy in the fight against terrorism. Available online: https://wcd.coe.int/ViewDoc.jsp?id=1469161 (last accessed 05.08.2012).

[65] Brown, I., Korff, D., Ibid., p. 5.

[66] Humans Rights Council, 2009, Ibid., cited supra note 13, p. 21.

[67] Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Human Rights Council, A/HC/13/37, p.21.

[68] For instance, in the United Kingdom, surveillance cameras are used during political protests and images are kept in a database. Polls show that because of this reason, one in three individuals are reluctant to participate in protests due to privacy issues.

[69] Humans Rights Council, 2009, Ibid., cited supra note 13, p. 22.

[70] Ibid., p. 21.

[71] This question has also been raised and discussed by the International Council of Human Rights Policy. For a debate on this issue See International Council of Human Rights Policy, 2011, Navigating the Dataverse: Privacy, Technology, Human Rights, Geneva, Switzerland, p. 25-34.

3.2 INCREASING SURVEILLANCE AND DATA PROFILING – THE MAIN TOOL IN COUNTERING TERRORISM

As we saw above, the right to privacy is not an absolute right. When States are monitoring terrorism activities, which represent a state of emergency threatening the life of a nation, privacy can be subject to limitations[72]. The fight against terrorism involves the need to collect systematically personal data and DNA data and to plug it into databases. According to some interpretations, this data collection is essential in order to comply to the UN resolutions for the prevention and repression of each typology of terrorist funding, as well as the freezing funds that are directly or indirectly used to that purpose[73].

Being a very complex environment, the Internet can be used for various terrorist purposes - such as propaganda, financing, training, planning, execution and other types of cyber-attacks.[74] Different networks can be used by terrorists as a means of communication between the "lone wolf" actors and larger networks of terrorists[75]. It has been shown that cybercrime has overpassed drug trafficking as a terrorist financing enterprise[76]. Identity theft, counterfeiting and other types of computer frauds seem to yield high profits under a shroud of anonymity[77]. According to press reports, grave terrorist attacks like the one in Bali, Indonesia, in 2002 were partially financed through online credit card fraud[78].

Therefore, in order to prevent terrorist acts, States often need to supervise Internet traffic. A significant part of the knowledge about the way terrorist groups function or where they target is obtained from different websites, chat rooms or other Internet communications. In the recent years, law enforcement entities and other intelligence institutions have developed

---

[72] As showed by the Special Rapporteur, once an individual is investigated or screened by a security agency, personal information is shared among security agencies for reasons of counter terrorism and therefore the right to privacy is affected. However, the Special Rapporteur showed that "countering terrorism is not a trump card which automatically legitimates any interference with the right to privacy".

[73] Foggetti, N., Ibid., cited supra note 41, p. 365.

[74] United Nations Office on Drugs on Crime, 2012, Ibid., cited supra note 3, p. 15-21.

[75] Theohary, C., Rollins, J., 2011, Terrorist Use of the Internet: Information Operations in Cyberspace, Congressional Research Service, p. 2. Available online: http://www.fas.org/sgp/crs/terror/R41674.pdf (last accessed 05.08.2012).

[76] Ibid., p.2.

[77] Ibid., p. 2.

[78] Sipress, A., 2004, An Indonesian's Prison Memoire Tales Holy War into Cyberspace, Washington Post, http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html (last accessed 05.08.2012).

sophisticated tools to prevent, detect and deter terrorist activities using the Internet. Among the most common strategies of domestic and foreign agencies to counter terrorism is the passive monitoring of website activities for intelligence purposes, engaging with other users in different chat rooms to elicit further information for counter-terrorism purposes or even the shutting down of websites[79]. There has also been a rapid development of "dataveillance", which includes monitoring of the data traits left by individuals when performing different transactions, computer readable facial photographs, fingerprints, DNA, medical records etc[80].

Many countries have introduced extraordinary laws and policies, which provide new surveillance powers to the State as a result of the increasing use of the Internet for terrorism purposes. For instance, in the European Union there are different mechanisms and law enforcement systems that collect data from individuals, among which Europol (a law enforcement organisation that handles criminal intelligence and whose aim is to combat serious international organised crime), Eurojust (a network of criminal-judicial authorities, which stimulates the coordination of investigations and prosecutions), Eurodac (a system which allows for the cross checking of fingerprints of asylum seekers and suspected illegal migrants), Schengen Information System (a system which counters the risks stemming from open borders by outputting lists of people classified as suspects), Visa Information System (exchange of visa information by Member States used to prevent, detect and investigate terrorist offences), Customs Intelligence Systems (used to help customs prevent, investigate and prosecute serious contraventions of national laws) etc[81].

Although in the USA and the UK many of the laws that provide surveillance powers have come to be questioned by legislative bodies, through the media, the courts and public sphere[82], in practice the legislations have still not yet accommodated in a comprehensive manner a balanced regime of the two rights. For example, the programme for intercepting telephone calls and e-mails authorised by the president Bush administration in 2001 and renewed in subsequent years, was ultimately considered a violation of the

---

[79] United Nations Office on Drugs on Crime, 2012, Ibid., cited supra note 3, p. 45.

[80] Ibid., p. 45.

[81] Hammarberg, T., 2008, Protecting the right to privacy in the fight against terrorism, https://wcd.coe.int/ViewDoc.jsp?id=1469161 (last accessed, 05.06.2012).

[82] See Foggetti, N., Ibid., cited supra note 41, p. 371.

First and Fourth Amendment of the US Constitution[83]. In particular, the District Court of Detroit noted that "it is not possible to pursue the goal of security by depriving citizens of constitutionally guaranteed rights"[84]. However, States are still far away from having adopted efficient legislations that also respond to the needs of international cooperation. Therefore, there is an urgent need to adopt clear standards that would provide an efficient setting for international cooperation between different States and organisations.

4. URGENT NEED OF CLEAR STANDARDS AND HARMONISED LEGISLATION

It is believed that global consistency on Internet privacy protection is important for many reasons: not only to boost the growth of electronic commerce[85], but also for the public safety and for countering of criminal activities using Internet related technology. In order to protect users in a globally consistent manner, legislation, self-regulation, technical solutions and combination solutions have to be implemented and addressed by States[86]. Firstly, the States need to find, agree upon and implement a balance policy regarding privacy and security, at least on a theoretical level. Then, the aim is to establish well defined standards and principles that would be accepted by the entire international community.

4.1 BALANCED POLICY IN RESPECT TO THE RIGHT PRIVACY AND RIGHT TO SECURITY

When it comes to the relationship between the respect of privacy and countering terrorism, Brown et al. claim that privacy and non-discrimination rights, which are at the core of many legal frameworks, are being challenged by the increased surveillance and profiling of terrorism suspects[87]. In the authors' view, there is a disproportional balance between the two rights and this is problematic for democracy and the rule of law, as this situation can lead to practical difficulties for cross-border cooperation between law enforcement agencies[88].

---

[83] Ibid., p. 374.

[84] Ibid., p. 374.

[85] Chung, W., Paynter, J., 2002, Privacy issues on the Internet, Proceedings of the 35th Hawaii International Conference on System Science, p. 1.

[86] Ibid., p. 1.

[87] Brown, I., Korff, D., 2009, Terrorism and the proportionality on internet surveillance, European Journal of Criminology, Vol. 6, No. 2., p. 1.

[88] Ibid., p. 1.

According to Golder et al., an efficient solution for assessing the counter-terrorism laws, from a human right perspective, is to adopt a "balancing approach", on the basis of which the importance of the relevant human rights, such as privacy, is weighted against the importance of the societal or community interests[89]. In this view, that we also share, human rights and national security can be reconciled through re-conceptualizing counter-terrorism legislation as "human security legislation" directed towards securing the necessary preconditions for the enjoyment of peace, prosperity, human well-being and human rights themselves[90].

States need to understand and agree on the limits that can be imposed to the respect of privacy. This can be, of course, a difficult task, as there are situations in which different rights conflict with others and it is sometimes impossible to decide which have to prevail. As depicted by Golder, on particular occasions, non-derogable rights will be in conflict with each other, such as in the ''ticking bomb'' scenario where the right to life may conflict with the right not to be subjected to torture[91]. In these cases the balancing approach will necessarily be engaged, and legislators and policy makers will have to outweigh the interest of one right against the other in attempting to ensure the least possible derogation from each[92].

According to the same author, if the decision maker is required to balance the importance of a non-fundamental right against community safety or national security, the decision maker should require the most cogent empirical evidence available that the proposed means of achieving the goal of community safety and national security will actually be effective[93]. The rule of balancing requires the decision maker to "justify the derogation of human rights by reference to a demonstrated link between the means (which derogates from the human right) and the end (community safety or national security)"[94]. For instance, in the context of a parliament legislating prospectively, this will require policy makers to make some attempts to forecast the social, political and economic effects of their proposed action[95].

---

89 Ibid., p. 1.

90 Golder, B., William, G., 2006, Balancing National Security and Human Rights: Assessing the Legal Response of Common Law Nations to the Threat of Terrorism, Journal of Comparative Policy Analysis, Vol.8, No. 1, p. 44.

91 Ibid., p. 55

92 Ibid., p. 55.

93 Ibid., p. 55.

94 Ibid., p. 55.

95 Ibid., p. 55.

But in many cases, according to Golder, "if the desired goal of national security and community safety can be achieved through means which do not derogate from human rights, then that is the legislative course that should be adopted"[96]. At the same time, the concept of proportionality requires the legislator or policy maker to consider and evaluate alternative means. In order to achieve successful implementation, "policy makers should be encouraged, before adding to the already long list of counter-terrorist legislation, to investigate options such as initiating community education, fostering meaningful cross-cultural, religious community dialogue or critically reviewing the social and economic effects of their foreign policies"[97]. This might seem difficult to achieve, especially since different countries relate differently to privacy and to what it entails. However, this endeavour could be the first step for adopting a set of well defined standards and principles that could be accepted by the entire international community.

4.2 WELL DEFINED STANDARDS AND PRINCIPLES FOR THE INTERNATIONAL COMMUNITY

Although it seems that the international community has already established mechanisms to address the issues related to terrorism, including the creation of the Counter-Terrorism Committee (CTC) and Counter-Terrorism Executive Directorate (CTED), it has not yet agreed on an universal definition of terrorism[98]. Without an universally agreed definition of terrorism[99], there is a danger that States may create broad, overreaching definitions and inadvertently criminalise outside the realm of terrorism. This is of a very high importance in determining how the Internet can be used for terrorism purposes and to which degree the activity on this virtual environment can be legally put under surveillance and controlled.

As pointed out by the United Nations experts, the problem resides in the fact that the areas of Internet regulation and content control are subject to

---

[96] Ibid., p. 57.

[97] Ibid., p. 58.

[98] Human Rights Advocates, Counter-terrorism and the protection of human rights, Human Rights Council: 13th Session, Agenda Item 3: Countering Terrorism, p. 4.

[99] The most comprehensive definition ids the one given by the European Union who defines the concept as "[the threat or act of] seriously intimidating a population, unduly compelling a Government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation." See Framework Decision 2002/475/JHA, Article 1.

many variations on national levels[100]. "Data protections in law and relevant human rights, even if they are adequate at national level, are rarely equipped for the transnational context in which data storage takes place"[101]. For example, UDHR and ICCPR provide international standards for the regulation of expression and communication of ideas[102]. However, in a publication of the UNODC, the experts put forward the fact that there is no comprehensive internationally binding instrument setting binding norms on what is considered appropriate Internet content or how States should regulate Internet-related activity within its territory[103]. In their view, the absence of a universally agreed definition of terrorism presents an ongoing obstacle to any internationally agreed approach to the appropriate regulation of terrorism-related activity over the Internet[104].

In order to efficiently fight terrorism, but also to ensure democracy and the respect for privacy, the States need to adopt clear standards for the collection, storage, use, analysis, disclosure and sharing of personal data for anti-terrorism purposes[105]. Since the Internet can be used for terrorist purposes on a global level (an act may be planned in one part of the world and executed in another), the rules on the matter must be binding to all States and the limits of statutory powers, as well as the unambiguous description of the kind of information, which may be recorded, must be clearly indicated[106].

The Special Rapporteur urges the States to assess how counter-terrorism laws, policies and practices that intrude on privacy are necessary and proportionate by implementing a range of principles.[107] According to him, the States should adopt in their policies the principle of minimal intrusiveness. On the basis of this principle, the governments should resist the tendency to collect more personal information or establish larger databases than needed

---

[100] United Nations Office on Drugs on Crime, cited supra note 3, p. 28.

[101] International Council of Human Rights Policy, 2011, Navigating the Dataverse: Privacy, Technology, Human Rights, Geneva, Switzerland, p.i. Available online: http://www.ichrp.org/files/reports/64/132_report_en.pdf (last accessed 05.08.2012).

[102] For more details See Mendel, T., 2011, Freedom of expression and broadcasting regulation, UNESCO, Brasilia Office, Brasil.

[103] United Nations Office on Drugs on Crime, cited supra note 3, p. 28.

[104] Ibid., p. 28.

[105] Brown, I., Korff, D., Ibid., p. 8.

[106] Ibid., p. 8.

[107] See Human Rights Law Research Centre Policy Brief, Protecting privacy while responding to terrorism. Available online: http://www.hrlrc.org.au/files/Policy-Paper-Protecting-Privacy-while-Countering-Terrorism1.pdf (last accessed 05.08.2012).

or to implement proposals for increased surveillance[108]. The Rapporteur also suggests the adoption of the principle of purpose specification restricting secondary use. By doing this, States must be obliged to provide a legal basis for the reuse of information, in accordance with constitutional and human rights principles[109]. This principle is of utmost importance when information is shared across borders. A third principle recommended by the Rapporteur is the principle of oversight and regulated authorisation of access, according to which surveillance systems require effective oversight to minimize harm and abuses[110]. He thus calls for the increased internal oversight to complement the process for independent authorisation and external oversight. The fourth principle, the principle of transparency and integrity, requires openness and communication about the surveillance practices[111]. Finally, the principle of effective modernization requires the States to introduce privacy impact assessment that articulates privacy considerations in the design of new surveillance techniques. The use of such types of tools as privacy impact assessment may help inform the public about the surveillance practices[112].

Showing that States no longer limit their exceptional surveillance schemes to combating terrorism and make these surveillance powers available for all purposes, the Special Rapporteur urges the States to develop and adopt international legal standards to ensure that privacy is respected and surveillance methods are not abused. He urges them to make sure that the surveillance is as unobtrusive as possible and that it is accompanied by authorization and regular reporting[113].

5. CONCLUSIONS

The main challenge of the present study was to examine the way data protection should be taken into account in the counter-terrorism strategy both on a global and regional level. As data protection is often considered an obstacle to effective counter-terrorism measures, basic international com-

[108] Humans Rights Council, 2009, Ibid., cited supra note 13, p. 28.

[109] Ibid., p. 28.

[110] Ibid., p. 29.

[111] Ibid., p. 29.

[112] Ibid., p. 30.

[113] Humans Rights Council, 2009, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development – Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, p. 31.

mitments providing for it are often not respected[114]. Consequently, the study aimed to encourage finding a balance between the right of security and the right to privacy, by keeping in mind that for the preserving of the democratic values, both of them are fundamental.

Nonetheless, another objective of the study was to show that States have an obligation to adopt a legal framework as a basis for any collection, storing, analysis, disclosure and sharing of personal data for terrorist purposes[115]. These rules need to be binding and must provide a precise description of the type of information that can be recorded, the categories of people against whom these measures can be taken, the circumstances that can lead for such a decision to be taken etc. Only by adopting a transparent legal framework, States will be able to ensure the rule of law in both the field of security and protection of human rights.

[114] Hammarberg, T., Ibid., cited supra note 63, p. 2.
[115] Brown, I., Korff, D., Ibid. cited supra note 85, p. 2.