UNIVERSITY OF TARTU
FACULTY OF LAW
Department of Public Law

Agnes Zaure

APPLICATION OF INTERNATIONAL HUMAN RIGHTS ONLINE- BALANCING PRIVACY, FREEDOM OF INFORMATION, AND NATIONAL SECURITY

Master thesis

Advisor
Dr.iur. EnekenTikk-Ringas
Co-advisor
Prof. Lauri Mälksoo

Tartu
2016

Table of content

Introduction

A transfer of electronic data by Internet users has contributed in a major way to the complexity of legal relations in an interconnected world. States are faced with the increasing doctrinalization of cyberspace challenges while constituting and exercising individual rights and freedoms. Recently, the United Nations resolution, stating that the same standards for the international human rights must be protected online, did not put to rest the tedious debate about the question of re-considering the position of civil liberties and national security established in international human rights treaties in times of continuous escalation of new emerging threats to national security.

This inevitable tension in the search for the compromise between polar views on the international human rights and national security has not been solved yet. As a result, the new emerging threats to national security and the relatively vague wording of binding international legal standards have led states to re-consider the balance of civil liberties and national security established in international human rights treaties and to start implementing at national level a number of new rules to create the legal ground for the increasing application of security measures online. The absence of a shared vision on the future of legitimate limitations of the human rights in favour of national security interests has resulted in a polar dichotomy between judicial, legislative and executive powers among States that endangers the existing understanding of democracy and the rule of law.

The controversy between State actors of the internet society stands at the crossroad: deciding whether it is possible to continue the application of the balance model according to the existing universal treaties in the light of changed national security needs, or not. Emerging case-law differs between regions, such as the EU, the US and the UK, with substantially divergent balances between privacy, freedom of information and national security. Discussion of these issues introduces both conservative and libertarian views where emphasis is tilted towards the view that there is no need to reinvent human rights, rather that existing standards must be interpreted according to the online challenges. On the other hand, there are States chiefly motivated not to ensure the ‘old’ human rights in an online environment and encourage for the ‘new’ human rights for the Internet age. During these debates, no answers have so far been presented for how to find a common balance between the parallel demands of privacy, freedom of security and national security in existing international legal instruments so that States would more likely follow them. As there is no specific international

treaty or convention on what are these minimum guarantees that should be followed for the sustainable promotion and protection of human rights and fundamental freedoms online, it is essential to provide recommendations on the balance between the parallel demands of privacy, freedom of security and national security in international legal instruments that more willingly will be accepted by the leading States.

In the light of these questions the thesis will propose a project for the balance to be followed by States aiming to diminish the polar dichotomy between the judicial, legislative and executive powers by establishing minimum standards for international human rights restrictions in the name of national security in the context of electronic data processing. For the purpose of achieving this aim, the thesis looks at the minimum scope of protection for international human rights in cyberspace and revises which legal expectations contained in international human rights treaties States must meet. Further, the thesis examines the balance of rights focused upon at the international level. For the next stage, the thesis intends to reveal regional implementations of national regulations and explore how these balances correspond to the international standards discovered above. For this reason, the thesis systematically explores the current practice of the most influential States and regions in global cyber security decision-making. If any contradiction is found, the thesis reveals the reasons that States used to justify a practise of online security measures contrary to the international treaties. If these reasons can be solved by international legal measures, the thesis proposes recommendations on potential solutions to achieve unity and clarity of balances for the rights and national security to be considered as relevant standards for future practice.

The thesis focuses precisely from the view of these rights as the most hotly so far debated human rights with respect to electronic communication online. The model for the triangular approach of the thesis originates from research papers[1] issued by ICT4Peace Norms Project for Hague Global Conference on Cyberspace. The thesis suggests seeing privacy, freedom of information, and national security as a complex concept of the interrelationship of all three aspects applicable in cyber matters which deserve closer study as a three-dimensional paradigm appearing in legal matters of electronic data processing. So far, the international courts in related matters have been focused mainly on a two-sided approach, instead of the approaching issues through the triangle of themes. The proposed approach is seen from the

[1]E. Tikk-Ringas. Norms for International Peace and Security: Privacy, Freedom of Information and National Security. ICT4Peace Norms Project. April 2015, p 3. - https://www.gccs2015.com/sites/default/files/documents/Working%20PaperPrivacy,%20Freedom%20of%20Information%20and%20National%20Security.pdf (16.02.2016).

following perspectives: the right to privacy, as a protection from extraction of information on individuals and contexts; the freedom of information, as part of freedom of expression, in the sense of the right to receive and impart information; and, in particular, national security, as in the security of nation states against man-made threats.

To achieve this aim, the thesis examines human rights standards set in the case-law of the European Court of Human Rights and the International Court of Justice, as well as selected regional regulations, regulatory trends and future prospects. The thesis concentrates on interpretations by the main treaty bodies of the United Nations system, as well as regional systems of European organisations. The interpretation of a particular right will be guided also by resolutions or general comments adopted on occasion by treaty bodies to give a fairly detailed guide. Most interpretation has been drawn through judgments or other forms of decision in a context of specific cases.

The thesis follows the logic of systematic analysis of those foremost questions in order to check the validity of the hypothesis raised up and also to achieve the final aim of research. The thesis opens by analysing the legal scope of protection for focused human rights: privacy and limits of free flow of electronic data transmitted via Internet facilities, as well as where courts have decided limitations are appropriate in favour of national security interests. In order to explore potential common denominators and shared attributes in the existing human rights instruments, the thesis will examine in the first chapter the legal scope of protection for each cornerstone of the triangle and find which circumstances can justify their limiting.

After discovering the normative standards, the relevant State practice will be examined to explore which model of balances States have been favouring. In cases of any disparities, the second chapter examines the extent of disparity between norms and States' practices. The obstacles to their interpretation and implementation will be analysed in the second chapter. If a major disparity is discovered, then for the purpose of answering the question on how the best to apply human rights in the context of rapidly developing information and communications technologies and what could be future standards and recommendations, the third chapter will analyse future solutions for those foremost questions.

Regarding methodology, for the purpose of examining the development of the balances before and after the terrorist attacks 9/11, in Madrid 2004 and London 2005, the historical research method is applied to see the shift in the national state regulations and relevant case-law. The

comparative method has been applied to reveal what can be the minimum common denominators of the human rights for the states to be considered as acceptable legal standards to be obeyed. Finally, the qualitative method has been applied to the relevant case-law analysis necessary to find out the judicial concept on the balance. The thesis relies also on an analytical and systematic approach to the respective case-law and legal documents study related to the tasks of thesis both on regional and national levels. In addition, and alongside the comparative and historical methods, synthetic methods will be used. The comparative method is used to reveal disparities between European legal standards in regulatory documents and the States' practices with their national regulations. The second chapter uses both systematic and synthetic methods. The historical method is used in case-law analysis to see whether there are fundamental differences between case-law before wide use of electronic communication and after.

The main sources used for the research are normative instruments and the authoritative commentaries by respectful legal scholars on international treaties, as well as commentative reports by political organisations and impartial rapporteurs that deserved respect to be reliable in respective discussions. Also, the thesis is based on relevant empirical case-law study of the national or regional courts. The European Union, the United States of America, the United Kingdom, and Russia are examined with regards to the compatibility of the national and the international legal standards of the human rights limitations. These States had the most attention as these are territories which are generally lauded for fulfilling commitment to the protection of human rights. These are also countries that have experienced challenges to their national security as a result of both foreign and domestic terrorism.

The human rights treaties themselves make no mention of the types of situations in which the provisions are to apply. However, it is evident from the wording of the 2012 UN Human Rights Council resolution[2] confirming that the same human rights that people have offline must also be protected online, thus, the resolution establishes protection of human rights in online as well.

[2] United Nations General Asembly. The right to privacy in the digital age. A/RES/68/167. 21 January 2014, para. Available: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.

A Scope of legal protection and limitations

I. Scope of legal protection for privacy, freedom of information and national security

For the purpose of better understanding the interrelations between respective human rights, it is essential to understand the core nature of these rights. This section focuses on interpretations by the main international treaty bodies of the United Nations and the European Union systems in cyberspace. A general interpretation is divided into subsections which represent the right to privacy from the international human rights law and the European law perspectives.

1. Right to privacy

a) Protection under the United Nations regulation

The UN secured the right to privacy in the Universal Declaration of Human Rights[3] (hereinafter UDHR) Article 12 (1) where the term "privacy" became an umbrella term[4] for privacy, family, home, correspondence, honour and reputation of individuals. It constitutes 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.*" In addition, seventeen years after drafting the UDHR, the provision on the right to privacy was worded in the Covenant on the Civil and Political Rights[5] (hereinafter ICCPR) Article 17 (1) which almost identically repeated the concept of the right to privacy in Article 12 (1) of the UDHR. The sole difference between those provisions consists in the legal base for restriction while the ICCPR prohibits also unlawful interferences to one´s privacy.[6]

Within the UN Guidelines Concerning Computerized Personal Data Files[7], adopted by the UN General Assembly, the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[8] are legal instruments addressing the protection of the

[3]The Universal Declaration of Human Rights. 1948.
[4]O. Diggelmann, M. Cleis. How the Right to Privacy Became a Human Right. -Human Rights Law Review 2014. No 14, p 447.
[5]The Covenant on the Civil and Political Rights, 1966.
[6] O. Diggelmann, M. Cleis, p 449.
[7]The UN Guidelines Concerning Computerized Personal Data Files. Doc E/CN.4/1990/72, 20.2.1990.-http://www.un.org/documents/ga/res/45/a45r095.htm, 14.12.1990.
[8] The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Paris 1980.-https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

privacy with regards to electronic data transfers. Thus, the United Nations (hereinafter UN) has acknowledged the protection of privacy regards to data transfers.

In 1988 the Human Rights Committee (hereinafter Committee), which is a monitoring body to implementation of Article 19 of the ICCPR, analysed the content of the right to privacy in its General Comment No. 16, according to which Article 17 aims to protect individuals from any unlawful and arbitrary interferences with their privacy, family, home, or correspondence, and national legal frameworks must provide for the protection of this right. This provision imposes specific obligations relating to the protection of privacy in communications, underlining that "correspondence should be delivered to the addressee without interception and without being opened or otherwise read. In relation to surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations, were prohibited.[9] Consequently, in 1980s the right to privacy in regulation was highly valued and protected and restrictions were considered exceptional. Both assured that the right to privacy involves the protection of separation from society.

Both international treaties provided an almost universal scope of protection, however some treaties, such as the African Charter on Human and People´s Rights,[10] Article 9 which uses for the right to privacy a different formulation. Despite the fact that the UDHR does not have directly binding effect on States, it is widely regarded as having acquired legal force as customary international law.[11]

In 17 April 2013 the UN General Assembly issued Report of the Special Rapporteur to the Human Rights Council[12] which argues that the right to privacy is a qualified right, but its interpretation raises challenges with respect to what constitutes the private sphere and in establishing notions of what constitutes public interest. Here the UN Special Rapporteur specified that privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without

[9]Centre for Civil and Political Rights (CCPR) General Comment No. 16. (General Comments), p 8.
[10]The African Charter on Human and People´s Rights, 1981.
[11]Article 19. The Johannesburg principles on national security, freedom of expression and access to information. November 1996, p 2.
[12]F.La Rue. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 17.04.2013. - http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/23/40 (16.02.2016).

interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.[13]

As the right to privacy is the ability of individuals to determine who holds information about them and how that information is used,[14] individuals must be also able to ensure that communications remain private, secure, and, if they choose, anonymous while exercising their right to privacy in communications. The UN Report on the privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself where security of communications means that individuals should be able to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion. Therefore, one of the most important advances enabled by the Internet is anonymity of communications which allows individuals to express themselves freely without fear of retribution or condemnation.[15]

b) Protection under the European Union regulation

Within the European Union region the right to privacy is guaranteed primarily by the European Convention for the Protection of Human Rights and Fundamental Freedoms[16] (hereinafter ECHR) which is binding upon Council of Europe states and which similarly to UN lays down the precise legal criteria of the protection of the right to privacy.[17] The first paragraph of Article 8 of the ECHR provides the content of the right to privacy by stating: "*Everyone has the right to respect for his private and family life, his home and his correspondence*".[18]

As mentioned above, despite the fact that private life has complex contours, pursuant to the case-law of the ECHT, Article 8 covers protection of individuals against attacks on honour and reputation, the use of a person´s name, identity, or likeness, being spied upon, watched, or harassed, and the disclosure of information protected by the duty of professional secrecy[19].

[13]F.La Rue. 2013, p 17.
[14]Lester and D. Pannick (Ed). Human Rights Law and Practice. London: Butterworth 2004, para 4.82.
[15]F.La Rue. 2013, pp 6-11.
[16]Convention for the Protection of Human Rights and Fundamental Freedoms. 1950.- http://www.echr.coe.int/Documents/Convention_ENG.pdf.
[17]P. Malanczuk. Freedom of Information and Communication. -Max Planck Encyclopedia of Public International Law. April 2011, para 47.
[18]The European Convention on Human Rights. 1950.
[19] C. Velu. The European Convention on Human Rights and the Right to Respect for Private Life, the Home and Communications. Cited in: R. White, C. Ovey. The European Convention on Human Right. 5th Ed., Oxford Univeristy Press, p 357.

Today the right to privacy involves protection of not only physical distance[20] from society, but also it shields the person against unwanted gazes from a distance, including from any forms of interception of electronic communications, which might include the opening of communications, Internet activity, or listening to telephone communications.[21]

The provision covered the right to privacy almost exactly copying UN treaty bodies in interpreting the right[22]. There is not much evidence on what drafters of the ECHR meant by the term "privacy" or "private life" as there are hardly any records of discussions of fundamental matters, such as aspects of privacy,[23] thus, the European Court on Human Rights (hereinafter ECtHR) has attempted a general explanation in numerous decisions on the scope of the protection of private life with regards to interference in electronic communications. Particularly, in *A v. France*, the ECtHR found that the use of covert technological devices to intercept private communications falls within the scope of Article 8 of ECHR as "*a telephone conversation does not lose its private character solely because its content concerned or might concern the public interest"* [24]. In addition, in *Halford v. the United Kingdom*, the ECtHR ruled that telephone calls made from business premises as well as from the home and intercepted by police, probably with the aim of gathering material to assist in the defence of proceedings, might be covered by the notions of "private life" within the meaning of Article 8.[25] As a contrast, where an applicant used a radio channel for civil aircraft, the interception did not constitute interference with private life since the conversation was on a wavelength accessible to other users and could not be classified as private communication.[26] Thus, the collection of private information by covert surveillance operators to find out about an individual without his consent will always concern his/her private life and will thus fall within the scope of Article 8.

Consequently, it might be concluded that the core nature of the right to privacy in online protection covers the protection of individuals against any attacks on honour and reputation, the use of a person´s name, identity, or likeness, without being spied upon, watched, or

[20]*Ibid*, p 458.
[21]Robin White, Clare Ovey. The European Convention on Human Right. 5. Ed. Oxford Univeristy Press: 2010, pp 365-366.
[22]O. Diggelmann, M. Cleis. How the Right to Privacy Became a Human Right. -Human Rights Law Review 2014. No 14, p 452.
[23]*Ibid*, p 457.
[24]ECtHR 14838/89, *A. v. France*, 23 November 1993, para 35.
[25]ECtHR 20605/92. *Halford v. the United Kingdom*, 25 June 1997, para 44.
[26]U. Kilkelly.The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights. Human rights handbooks, No. 1. Directorate General of Human Rights Council of Europe. 2003, p 13.

harassed, and the disclosure of information protected by the duty of professional secrecy. Thus, any activity online concerning an individual´s data transmission via Internet is included to the protection of the private sphere.

2. Freedom of information

a) Protection under the United Nations regulation

Since 1946, the freedom of information was recognised as a fundamental human right at the UN General Assembly, in Resolution 59 (I) of 14 December 1946, in particular, by the US, the UK, and France who convened at the initiation.[27] Legal guarantees for the freedoms of opinion, expression, and information in the universal treaties, such as Article 19 of the UDHR, as well Article 19 (2) of the ICCPR, became universally recognised.

Article 19 (2) of the ICCPR provides that: "*Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*" Under Article 19 of the UDHR: "*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers*". There is no universally agreed legal definition of the freedom of information provided by either the UDHR or the ICCPR, but the freedom of information has been recognised as subcategory of the freedom of expression.[28]

The UN General Comment No 34 on freedom of opinion and expression[29] affirms that under the UN all forms of expression and the means of their dissemination are protected. Such forms include spoken, written and sign language and such non-verbal expression as images and objects of art. Means of expression include books, newspapers, pamphlets, posters, banners, dress and legal submissions. They include all forms of audio-visual as well as electronic and internet-based modes of expression.

[27]P. Malanczuk. Freedom of Information and Communication. -Max Planck Encyclopedia of Public International Law. April 2011, para 5.
[28]*Ibid*, para 21.
[29]General Comment No 34 on freedom of opinion and expression 2011. UN Human Rights Committee. CCPR/C/GC/34, para 11. http://www.ohchr.org/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf (14.02.3016).

Further on, in 2013, it has been affirmed by the UN Special Rapporteur Frank La Rue[30] that the freedom of information is fully applicable to the Internet. In 2011 the Special Rapporteur emphasized that Article 19 of the UDHR and the ICCPR was drafted with foresight to include and to accommodate future technological developments.[31]

It is beyond the scope of the present thesis to enter into a full discussion of the various aspects of the questions concerning the right of access to information held by public bodies (incl. intelligence services, or other entities when such entities are carrying out public functions). They are excluded from attention as they do not directly relate to the triangular scope of the privacy, freedom of information and national security interests. But it should at least be noted that respective principles have been adopted in relevant freedom of information laws which are drawn up and endorsed by a group of international law experts in the UN documents. Also, cases where disclosed private information by private individuals became public according to their deliberate will, are also left out of discussion, as there should be no dispute over privacy protection.

b) Protection under the European Union regulation

The right to freedom of information is guaranteed in all 47 member states of the Council of Europe.[32] In the EU region the right to freedom of information is guaranteed primarily by the ECHR Article 10 (1) which lays down that "*Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers*".

The content of the right has been explored in *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom*[33] and *10 Human Rights Organisations and Others v. the United Kingdom*[34], where the ECtHR has affirmed[35] that Article 10 of the ECHR is fully applicable

[30]F.La Rue. 2013, p. 23.
[31]Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/17/27. - http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/17/27 (16.02.2016).
[32]D. Voorhoof. The Right to Freedom of Expression and Information under the European Human Rights System: Towards a more Transparent Democratic Society. RSCAS 2014/12 2014. Robert Schuman Centre for Advanced Studies Centre for Media Pluralism and Media Freedom, p 1. - http://cadmus.eui.eu/bitstream/handle/1814/29871/RSCAS_2014_12.pdf?sequence=1 (16.03.2016).
[33]ECtHR *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom*, 62322/14, 11 September 2014.
[34]ECtHR *10 Human Rights Organisations and Others v. the United Kingdom*, 24960/15, 20 May 2015.
[35]European Court of Human Rights. New technologies. Factsheet. September 2014. - http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf. (18.12.2014).

to the Internet. In *Raichinov v Bulgaria*,[36] the ECtHR stated that freedom of expression is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb.[37]

ECtHR has explained[38] that the freedom of expression applies not only to the content of information but also to the means of its dissemination, since any restriction imposed on the latter necessarily interferes with the right to receive and impart information. Within the scope of the ECtHR the freedom of expression and information applies to the various forms and means in which information is transmitted and received, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.[39] The analysis of jurisprudence of the ECtHR allows us to conclude that Internet related disputes undoubtedly fall within the scope of the right to information privacy.

In conclusion, the protection of the freedom of information relates to all kinds and sorts of expression and the means of their dissemination, whether spoken, written and sign language and such non-verbal expression as images in books, newspapers, pamphlets, posters, banners, dress and legal submissions via Internet. Expressions do not have to please the audience, as under the freedom of information expressions that offend, shock, or disturb are also protected on the Internet.

3. National security

a) Protection under the United Nations regulation

National security interests entail a need for States to protect their governmental structure, public order and rules of enforcement mechanisms.[40] Almost all laws are created to protect the basic interests of States and to provide legal grounds for acting in favour of creating these interests despite individual human rights.[41] The UN secured[42] the interests of national security as an exception that should be read according to the meaning of previous paragraphs of the same article. This way, the rule for applying national security should be interpreted by reading

[36]ECtHR *Raichinov v Bulgaria* 47579/99 20, April 2006, para 47.
[37]ECtHR *Observer and Guardian v. the United Kingdom* 13585/88, 26 November 1991, para.59-60.
[38] ECtHR *Case of Ahmet Yildirim v. Turkey* 3111/10, 18 December 2012, para 50.
[39]ECtHR *Autronic AG v. Switzerland* 12726/87, 22 May 1990, para 47; ECtHR *De Haes and Gijsels v. Belgium* 19983/92, 24 February 1997, para 48.
[40]K. Holmes. What is National Security? Index of US Military Strength 2015. - http://index.heritage.org/military/2015/important-essays-analysis/national-security/ (18.12.2014).
[41]I. Cameron. National Security and the European Convention on Human Rights. Iustus Förlag: 2000, p 40-49.
[42]*Ibid*, p 49.

the whole Article 19 of the ICCPR. Specifically, Article 19 (3) (b) provides that the exercise of rights indicated in the article carries with it special duties and responsibilities and may be subject to restriction, such as national security, except in cases where it is provided by law and is necessary.

At the current time the most relevant restrictions to individual rights in the electronic data protection context are in line with "national security", as"public order", "public safety", "the prevention of disorder or crime", and "the rights and freedoms of others" fall out of the scope of research as, for the benefit of this research, the focus is set on national security interests. Even if justifications for the restrictions to individual rights in protection of national security usually are based on complex reasoning which includes merely all purposes, such as listed above regarding counter-terrorism measures[43], the legal analysis on the system of rights limitations would be analogous for all listed grounds.

The "national cyber security" term entails non-definable denominators which are rapidly changing and do not have static characteristics in cyber matters. Also, these constructions might work for interstate incidents but not where individuals are involved. A closer look at definitions shows that the state of protection is never measured, never certain and always contains contradictions. Also there is no guidance as to whose interests and criteria are considered. Therefore, restrictions for national cyber security could be applied in very broad circumstances where a judge considers that the interests of any party are endangered in a way that may affect national interests.

Like national security, the concept of national cyber security is changing in accordance with a government's role and place in current time[44], its national values, interests and goals, means and methods preventing and reflecting internal and external threats, as well as the basis of organisation and principles of systems functioning to grant national security. As cyberspace looks like the systematic sphere of our life, national cyber security can be seen as cross-section of economic, social, political, military, spiritual-cultural, etc. fields of security where information systems can have a major effect.

[43]L. Doswald-Beck. Human Rights in Times of Conflict and Terrorism. Oxford: Oxford University Press 2011, p 415.
[44]F. Wamala. ITU National Cybersecurity Strategy Guide. September 2011, pp 42-43. - http://www.itu.int/ITUD/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (18.12.2014).

As there is no universally agreed positive definition on what constitutes national security or closely related terms such as “internal security” or “state security”, they vary from State to State. There are some States that have defined national security on a regional level, including Sweden in its Criminal Code, Hungary in Act CXXV of 1995 on National Security Services, Spain in the National Defence Act of 2005, the United Kingdom in the Security Service Act 1989, and Italy, which provides it by deduction specifically regarding the state secrets privilege from Article 39 (1) of Law 124/2007.[45]

To compare European legal systems to American, the European ones are designed to ward off two types of threats: domestic and foreign. In the United States, national security is perceived mostly as security from foreign powers abroad, not from internal threats, and especially not from home-grown internal threats. On the bureaucratic level, there are no domestic counterparts to the country's foreign intelligence agencies—the Central Intelligence Agency (the "CIA") for human intelligence and the NSA for signals intelligence. By the Inter-American Court concept, national security involves issues that address defence and protection of the secret services.[46] Even so, these issues of secret service, as related to the comments of army, secret military information policy, freedom of expression issues of journalists employed for the national intelligence services, etc., do not fall within the aim of the thesis as these issues are intimately related to the military field and deserve more focused and independent research than the current research has been aiming for.

It should be mentioned that a subcategory of national security is national cyber security[47], that it is closely linked to informational society security, and therefore should be viewed together with it. Comparing the UK Cyber Security Strategy (2011), the US Department of Defense Cyber Strategy (2015), and the draft of the Concept of Russia’s Cyber Security Strategy (2014), we cannot find any interpretation of national cyber security. All three strategies refer to the point that national cyber security protection objects are information and the means of its transmission and that has both a direct and indirect affect on the results of individual´s, organisation´s and government´s activity (economical, political, military etc.). Additionally,

[45]S. Coliver. National Security and the Right to Information. 11 December 2012, p 6. -https://www.opensocietyfoundations.org/sites/default/files/coliver-nsp-pace20121220.pdf (18.12.2014).
[46]L. Doswald-Beck. Human Rights in Times of Conflict and Terrorism. Oxford: Oxford University Press 2011, p 415.
[47]K.Ziolkowski (Ed). Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. Tallinn: NATO CCD COE Publication 2013, p 21. See also: The Cyber Index International Security Trends and Realities. UNIDIR/2013/3. New York, Geneva: United Nations Institute for Disarmament Research 2013. -http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (18.12.2015).

the components are national, social, and personal values which might affect State territory, nation and jurisdiction. Indirectly, the components might be a system of dissolution, use and construction of information resources within a State, or a system of construction of the nation´s public consciousness which is based on the use of mass communication. Based on compared strategies we can deduce the States´ need to adopt a new cyber security strategy every 4-5 years, reflecting changing needs and priorities of governments in a fast developing informational technology and therefore, the concepts of national cyber security.

b) Protection under the European Union regulation

The ECHR establishes restrictions to human rights as exceptions when used to protect national security, public order, defence or public safety. There is no definition of national security in the European legal instruments. National security is an object to be measured and scaled. In the results of public discussions, a compromise on national security interests reflects the part of a security which is agreed on by national authorities.

Same as on the UN level, the EU legislation does not provide the definition of security of the state and community against threats to their wellbeing. The term itself has been hopelessly expansible, and has in fact assumed more of an international-security dimension in the global war on terror[48] as well as conter-espionage, counter-terrorism and counter-subversion dimensions. This latter feature still survives in the legislation setting out the powers of the security service even though the anti-subversive unit of the security was wound up in 1992.[49] Global terrorism, the possible re-emergence of a cold war, and the globalisation of organised crime dictate the necessity. Cyberterrorism, cybercrime and cyberpornography pose major threats to government and society. North Korea, Burma, Cuba, Saudi Arabia, Iran, [50] China,[51] Syria, Tunisia, Vietnam, Turkmenistan,[52] have sought to censor by various devices the information that can be retrieved online. The blogosphere and Twitter have the capability to thwart the most restrictive of injunctions issued by courts against the press.[53] Governments

[48]*Secretary of State for the Home Department v. Rehman*, 2002.- http://www.1cor.com/1315/?form_1155.replyids=489.
[49]P. Birkinshaw. Freedom of Information: The Law, the Practice, and the Ideal. Cambridge: Cambridge University Press. 4. Ed. 2010. p 35.
[50] N. Akhavan. Electronic Iran: The Cultural Politics of an Online Evolution. Rutgers University Press. 2013, p 37.
[51]L. Zhou. Chinese cyber regulators are getting personal.-Business Insider 4.02.2015. - http://www.businessinsider.com/chinese-cyber-regulators-are-getting-personal-2015-2?IR=T (18.04.2015).
[52]Top 10 Internet-censored countries. -USA Today 5.02.2014. - http://www.usatoday.com/story/news/world/2014/02/05/top-ten-internecensors/5222385/.
[53] Patrick Birkinshaw, p. 11.

have increasingly taken steps to prevent the transmission of „obscene" material via the Internet.

According to the Vienna Convention on the Law of Treaties, the principle of interpreting any exceptions narrowly draws attention to the restrictive interpretation of the notion of "national security" with a requirement for Member States to refrain from intruding upon EU competences.[54] Consequently, the concept of national security entails protection of State´s national values, interests and goals, means and methods preventing and reflecting internal and external threats, as well as the basis of organisation and principles of systems functioning to protect them from foreign powers.

II. System of limitations

1. General requirements

As was noticed above, human rights, including privacy and freedom of information, are not absolute: they are subject to certain "formalities" or "conditions", *id est* restrictions. Requirements for balancing competing values are prescribed by control test where any restriction in favour of another value should be tested under the guidance provided in relevant case-law for measurement of proportionality of exceptions. Interferences are only allowed under the strict conditions that any restriction or sanction must be 'prescribed by law,'[55] must have a 'legitimate aim' and finally and most decisively, must be 'necessary in a democratic society.'

Under Article 10 (2) of the ECHR public authorities have a mandate to interfere with freedom of information by way of formalities, conditions, restrictions and even penalties. Therefore, an interference is legitimate if it is "prescribed by law", is pursuant to one or more of the legitimate aims set out in paragraph 2 and is "necessary in a democratic society" to achieve these aims. In addition, one of the requirements of expression "prescribed by law" is the ability to foresee in regulation the measure concerned. A regulation is regarded as a "law" if it is formulated with sufficient precision to enable a person to regulate his conduct. A person must be able to foresee, to a degree that is reasonable in the circumstances, the consequences

[54]C. Moraes. Draft Report on the US NSA surveillance programme. European Parliament. No 2013/2188(INI). 8.01.2014, p 9.

[55]In only a few cases the ECtHR came to the conclusion that the condition "prescribed by law," - which includes foreseeability, precision and publicity or accessibility and which implies a minimum degree of protection against arbitrariness, was not fulfilled, such as in ECtHR *Herczegfalvy* v. *Austria* 10533/8324, September 1992; ECtHR *Steel and Others* v. *UK* 24838/94, 23 September 1998; ECtHR *Hashman and Harrup* v. *UK*, 25594/94, 25 November 1999; ECtHR *Gaweda* v. *Poland*, 26229/9514, March 2002 and some others.

which a given action may entail. An appropriate advice may be applied to the person if need be.[56]

The degree of precision depends, to a considerable extent, on the content of the instrument at issue, the field it is designed to cover, and the number and status of those to whom it is addressed.[57] A law which confers a discretion, is not, in itself, inconsistent with the "prescribed by law" requirement, provided that the scope of the discretion and manner of its exercise are indicated with sufficient clarity to give adequate protection against arbitrariness.[58] So, if extensive interpretation is not founded on any legal provision which clearly authorised it and is not reasonably foreseeable for the citizen, it does not meet the "quality of law" standard under the ECHR.[59]

Whilst certainty is desirable, precision may bring in its train excessive rigidity, but the law must be able to keep pace with changing circumstances. For this reason, general provisions of law can at times make for a better adaptation to changing circumstances than can attempts at detailed regulation.[60] Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague, and whose interpretation and application are questions of practice.[61] But the dangers inherent in prior restraints call for the most careful scrutiny.[62]

Therefore, regulations on Internet matters at national levels should be able to provide a delineated understanding and clarity that helps to define limits for State responsibility and non-State actors and also to promote legal certainty. The ECHR has reiterated in this context that it is not its task to take the place of the domestic courts but rather that the ECHR is satisfied that provisions along with the pertinent case-law give clear guidance on proper behaviour.

An interference must also pursue a legitimate aim in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the

[56]ECtHR *Rekvényi v. Hungary*, 25390/94, para 34; ECtHR *Goussev and Marenk v. Finland*, 35083/97, para 53, 17 January 2006; ECtHR *Štefanec v. the Czech Republic*. 75615/01, para 44, ECtHR *Delfi vs Estonia* case 18 July 2006, § 71, p 17.
[57]ECtHR *Groppera Radio AG and Others v. Switzerland*, judgment of 28 March 1990, Series A no. 173, p. 26, § 68.
[58]ECtHR *Goodwin v. the United Kingdom*, 17488/90, 27 March 1996, para 31.
[59]ECtHR *Dzhavadov* v. *Russia*, 30160/04, 27 September 2007, para 40.
[60]ECtHR *Times Newspapers Ltd v. the United Kingdom*, 3002/03 and 23676/03, paras 20, 21 and 38.
[61]ECtHR *Lindon, Otchakovsky-Laurens and July v. France*, 21279/02 and 36448/02, para 41.
[62]ECtHR *Observer and Guardian v. the United Kingdom*, 26 November 1991, para 60.

disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. This list is exhaustive yet its interpretation and scope evolves with the case law of the courts. Moreover, the ECtHR evaluates whether the reasons adduced by the national authorities to justify interference, are "relevant and sufficient". For achieving its aims, the ECtHR has to assure itself that the national authorities applied standards which are in conformity with the principles embodied in the first paragraph of right, and that they relied on an acceptable assessment of the relevant facts.

In *Delfi vs Estonia*[63] the rights under Article 10 of the owner of a news portal were excessively restricted by holding it liable for comments written by third parties. Restrictions related to freedom of expression are considered proportionate when they, among others, pursue a legitimate aim of protecting the reputation and rights of others. In the ECHR's view the fact that the actual authors were also in principle liable does not remove the legitimate aim of holding the news portal company liable for any damage to the reputation and rights of others.[64]

There are fundamental principles concerning the question of whether an interference with freedom is "necessary in a democratic society".[65] Any restrictions to human rights under the ECHR Article 10 mechanism are connected to the requests of pluralism of views, tolerance and broadmindedness which serve as a cornerstones to the "democratic society". According to *MGN Limited v United Kingdom*, necessity within the meaning of ECHR implies the existence of a "pressing social need". The States have a certain margin of appreciation in assessing whether such need exists, but this need is operated under European supervision that covers both legislation and the decision applying, even those given by an independent court.[66]

As regards the meaning of the adjective "necessary" in Article 10 (2), the ECtHR confirmed in the case of *MGN Limited v United Kingdom* in its judgment of 18 January 2011 that it "impliesthe existence of a pressing social need". The States have a certain margin of appreciation in assessing whether such a need exists, but it goes hand in hand with

[63]ECtHR Delfi AS v. Estonia, 64569/09, 10 October 2013.
[64]*Ibid*, para 77.
[65]ECtHR *Hertel v. Switzerland*, 25 August 1998, para 46; ECtHR *Steel and Morris v. the United Kingdom*, 68416/01, para 87; ECHR *Mouvement raëlien suisse v. Switzerland*, 16354/06, para 48; ECHR *Animal Defenders International v. the United Kingdom*, 48876/08, para 100, 22 April 2013.
[66]P. Malanczuk. Freedom of Information and Communication. -Max Planck Encyclopedia of Public International Law. April 2011, para 50.

supervision, embracing both the legislation and the decision applying it, even those given by an independent court. [67]

The ECtHR have ruled that considered values should be treated with equal respect and that national authorities have to follow the requirement of fair balancing when two protected rights guaranteed by the ECHR are in conflict with each other in certain cases[68].

2. Privacy vs Freedom of Information

When finding a proper balance for the privacy and freedom of information, as a matter of principle, the rights guaranteed under Articles 8 and 10 deserve equal respect as it is recognized that the exercise of the right to privacy is important for the realization of the right to freedom of information and is one of the foundations of a democratic society.[69]

The Article 8 (2) of the ECHR sets conditions for limitations to the privacy right with the wording: "*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 wellbeing 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*". Article 10 (2) sets the legal conditions for the limitation of the freedom of information. It states: "*The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary*."

As for the notice, the questions of the protection of public figures' reputations and freedom to disseminate information will be left out of scope due to the main purpose of the thesis to focus on privacy, free flow of information online and national security.

[67] *Ibid*, para 101.
[68] ECtHR *Hachette Filipacchi Associés v. France,* 71111/01, para 43, 14 June 2007; ECtHR *MGN Limited v. the United Kingdom,* 39401/04, para 142, 18 January 2011; ECtHR *Axel Springer,* 39954/08, February 2012, para 84.
[69] United Nations General Assembly. Brazil and Germany: The right to privacy in the digital age. Draft resolution. November 2013, p. 1.

The right to privacy is justified to limits for the protection of the rights and freedoms of others. Where the right to freedom of expression is being balanced against the right to respect for private life, the relevant criteria in the balancing exercise include the following elements: contribution to a debate of general interest, how well known the person concerned is, the subject of the report, the prior conduct of the person concerned, the method of obtaining the information and its veracity, the content, form and consequences of the publication, and the severity of the sanction imposed.[70] Conclusively, according to the *Delfi vs Estonia* and *Von Hannover v. Germany* cases of the ECHR, the relevant criteria in the balancing exercise include the following elements: contribution to a debate of general interest, how well known the person concerned is, the subject of the report, the prior conduct of the person concerned, the method of obtaining the information and its veracity, the content, form and consequences of the publication, and the severity of the sanction imposed.[71]

Restrictions related to freedom of expression came into play in connection to rights under Article 8 of ECHR[72] in a lively lasting debate over the right to be forgotten that has been contested within the jurisdiction of ECtHR. Thus, in *Google Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD)*[73] the ECtHR acknowledged that EU citizens have the right to request internet search engine Google to remove search results directly related to them. This assessment balanced the interest of the person making the request and the public interest to have access to the data by retaining it in the list results.[74]

For the cases of reputation harm, for example if an attack on a person's reputation has attained a certain level of seriousness[75] and was made in a manner causing prejudice to personal enjoyment of the right to private life, the ECHR stated in *A. v. Norway* and *Axel Springer AG v. Germany* that the State authorities have a duty to strike a fair balance when protecting two values which may come into conflict with each other in certain cases.

[70]ECtHR *Delfi vs Estonia*, para 82; ECtHR *Axel Springer AG*, para § 87; ECtHR *Von Hannover v. Germany* . 40660/08 and 60641/08, para 106; ECtHR *Timciuc v. Romania*, 28999/03, para 144, 12 October 2010; and *Mosley v. the United Kingdom*, 48009/08, 10 May 2011, para 111.
[71]ECtHR *Mosley v. the United Kingdom*, 48009/08, para 111, 10 May 2011.
[72]ECtHR *A. v. Norway*, 28070/06, para 64, 9 April 2009; *Axel Springer AG v. Germany*, 39954/08, para 83, 7 February 2012.
[73]ECtHR *Google Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD)*, C-131/12, para 98, 13 May 2014.
[74]Myth-busting: The Court of Justice of the EU and „the right to be forgotten", p 4.
[75]ECtHR *Chauvy and Others*, para 70; ECtHR *Pfeifer v. Austria*, 12556/03, para 35, 15 November 2007; ECtHR *Polanco Torres and Movilla Polanco v. Spain*, 34147/06, para 40, 21 September 2010.

Consequently, the ECtHR has established the balance for the means with which citizens exercise their right to defend their interests, and in Europe the search engine operators act under the supervision of national data protection authorities which are legally required to perform an independent control. This author takes the view that the tendency of the ECtHR to put individuals back in control by updating their data protection rights can be followed and that there is no ground for spreading the idea that the ECtHR allows for massive censorship[76].

3. Freedom of Information vs National security

Privacy and security matters approach delicate content control regulation questions. There are many cases where the balance between freedom of information and national security has been struck, as enquirers have frequently been confronted with a number of obstacles, often with regard to a reluctance by the authorities to carry out their duty to investigate the facts adequately. Allegedly, public authorities have refused to disclose information in order to protect national security concerns[77] or for the effectiveness of their work. Still there are cases where access to certain types of information is limited and even the courts have been reminded of their limited role when accessing questions concerning executive judgments involving national security.[78]

For the balance between the freedom of information and national security, the ECtHR has been consistent about the relationship between civil liberties and national security. In *Rehman v Secretary of State*[79] the ECtHR ruled that the individual rights prevail over national security interests. The concept was introduced in *Malone v Metropolitan Police Commissioner* where the ECtHR found that the right of individuals are not subordinated to national security interests.

Technological surveillance for security purposes in public places has become an ordinary incident of life in many situations, but questions may arise as to the use made of the material recorded. In *Peck v. United Kingdom*[80] the distinction between the ordinary incidents of social living and a serious interference with respect to a person's private life in this context are

[76]Myth-busting: The Court of Justice of the EU and „the right to be forgotten", p 4.
[77]F. La Rue, para 20.
[78]P. Birkinshaw, p. 33.
[79]ECtHR *Rehman v Secretary of State*, 11 October 2001. *-http://www.publications.parliament.uk/pa/ld200102/ldjudgmt/jd011011/rehman-1.htm.*
[80] *Peck v. United Kingdom*, 36 EHRR 41, 28 Jan 2003.

illustrated.[81] Similarly, in *Malone v Metropolitan Police Commissioner* the ECtHR stated that human rights must prevail over national security interests. In *R (B.Mohamed) v Secretary of State for foreign and Commonwealth Affairs*[82] the Divisional Court ordered disclosure of documents by the UK government concerning details of torture on the claimant which were held by the US government subject to public interest certificates which the UK government was asked to clarify. The US government alleged that disclosure would prejudice intelligence relations between the US and the UK. In *Animal Defenders International v. the United Kingdom*[83], the ECtHR has also held that when a non-governmental organisation is involved in matters of public interest, such as the present applicant, it is exercising a role as a public watchdog of similar importance to that of the press.

Through these examples it became evident that, in the balance for the freedom of information versus national security interests, the ECtHR continue with the approach that national security interests can be considered as an appropriate restriction to the human right only in those cases where interference with human rights was justified by passing a «triple» control test of necessity, legitimacy and proportionality by means of lawful limitations.

1) Hate speech and war propaganda regulation

The ICCPR Article 19 does not protect speech inciting hatred, violence, and discrimination, and by support of Article 20 (1) and (2) of the ICCPR, the UN Human Rights Committee stresses that "acts addressed in Article 20 of the ICCPR, are of such an extreme nature that they are subject to restriction pursuant to the Article 20 (3)[84]." But the fine line between those expressions without any seriousness set out in Article 20 (3) [85] to the acts with systematic intentions to impose threat to the State sovereignty has been noticed.

Also, the prohibition of the "propaganda of war" under the Article 20 (1) has been addressed by the UN Human Rights Committee with "any propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law", but this provision does not prohibit advocacy of the

[81]R. Toulson. Freedom of expression and Privacy. Vol 41. Issue 2. London: 2007 (Paper presented at Association of Law Teachers Lord Upjohn Lecture. London. 9.02.2007), p 149.
[82]Administrative Court, Decision of England and Wales High Court, *Mohamed, R v Secretary of State for Foreign & Commonwealth Affairs*, CO/4241/2008, 21 August 2008.
[83]ECtHR *Animal Defenders International v. the United Kingdom*, 48876/08, para 103, 22 April 2013.
[84]General Comment No 34 on freedom of opinion and expression 2011, para 52.
[85]*Ibid*, para 54.

sovereign right of self-defence or the right of peoples to self-determination and independence in accordance with the Charter of the United Nations[86].

2. Restrictions on anonymity and encryption

In an age of pervasive online surveillance, questions of anonymity and encryption closely relate to the free flow of information, privacy and national security, are not prescribed in any international human rights instrument. Nevertheless, the anonymity and encryption must be objects of the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds; and must conform to the strict tests of necessity and proportionality.

In fact, that anonymity has been as a safeguard and advancer to privacy, free expression, political accountability, and public participation in debates. There are very few States that provide general protection in law for anonymous expression. However, although a number of States exert significant pressure against anonymity offline and online, there are several States' judiciaries who have protected anonymity, at least in limited instances: in 2014 the Supreme Court of Canada annulled the warrantless acquisition of an anonymous online user identity[87].

An extensive number of laws in countries around the world promote the effective use of both encryption and anonymity tools. Among them are Brazil with the Marco Civil da Internet Law (2014), Austria with the E-Commerce Act and Telecommunication Act, and Greece, Germany, Ireland, Norway, Sweden, and Slovakia, as well as the United States of America, encourage the use of encryption.[88]

Nonetheless, on the UN level States are urged to provide alternative recourses and other less intrusive means than disproportionate restrictions to freedom of information and privacy by the means of prohibition of anonymity and encryption. It is left up to States by which means to achieve solutions in a dilemma when their obligation to protect freedom of expression is in conflict with their obligations to prevent violations of the right to life or bodily integrity, which are put at risk by terrorism and other criminal behaviour. So far, the requests the disclosure of encrypted information through judicial warrants, by assuring that general

[86]General Comment No 11 on prohibition of propaganda for war and inciting national racial or religious hatred 1983, UN Human Rights Committee, para 2. - http://www.ohchr.org/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf (15.03.2016).
[87]*R.* v. *Spencer*. 2014.
[88]David Kaye. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. A/HRC/29/32. 22 May 2015, para. 38.

limitations on the security provided by encryption are necessary and proportionate, by showing publicly and transparently that other less intrusive means are unavailable, and that only backdoors would achieve the legitimate aim.[89] The anti-anonymity laws were declared as unconstitutional by the Constitutional Court of the Republic of Korea[90] Both, the ECHR and the Court of the United States protect the right to anonymous expression.[91]

On the other hand, there are numerous national regulations that prohibit anonymous speech online. Brazil, the Bolivarian Republic of Venezuela, Vietnam,[92] the Islamic Republic of Iran, Ecuador,[93] and the Russian Federation published separate regulations that would require users to provide identification to connect to networks[94]. These governments around the globe are working to restrict methods of anonymity and are seeking to undermine these obstacles to surveillance, potentially making the internet less secure for everyone.[95]

4. National Security vs Privacy

Further, let's have a look at the balanced approach between national security and privacy. The *Peck v. United Kingdom*[96] case points out the distinction between the ordinary incidents of social living and a serious interference with respect for a person´s privacy. The case emphasised that the disclosure of the images of closed-circuit television footage, which resulted in images of applicant being published and broadcast widely to the media, resulted in a breach of Article 8 of the ECHR by the reason that the applicant was in a public street but that he was not there for the purposes of participating in any public event, nor was he a public figure. The court recognised that the Council could have taken steps to obtain the applicant's prior consent to disclosure, it could have itself masked the images before making them available to the media, or it could have taken the utmost care in ensuring that the media to which the disclosure was made masked the images.[97] The ECtHR noted that the Council did

[89]David Kaye, para. 43.
[90]Decision 2010 Hun-Ma 47, 252, 28 August 2012. Cited in: D. Kaye, para. 47.
[91]US Supreme Court, *McIntyre* v. *Ohio Elections Commission*,1995, pp 342 and 343.
[92]Freedom House. Vietnam: freedom of the press. -https://freedomhouse.org/report/freedom-press/2015/Vietnam, 2015.
[93]S.Kelly, M.Earp, L.Reed, A.Shahbaz, M. Truong. Freedom on the Net 2015. Privatizing Censorship, Eroding Privacy. - https://freedomhouse.org/report/freedom-net-2015/freedom-net-2015-privatizing-censorship-eroding-privacy.
[94] Human Rights Watch. Human Rights Watch Submission: World Development Report on Internet for Development. -https://www.hrw.org/news/2015/08/26/human-rights-watch-submission-world-development-report-internet-development, 26.08.2015.
[95]Ecuador. Freedom on the Net 2014. Organic Law on Communications 2013. - https://freedomhouse.org/sites/default/files/resources/Ecuador.pdf.
[96]ECtHR *Case of Peck v. the United Kingdom,* 44647/98, 28 January 2003, para 111.
[97]Ibid, para 80.

not explore the first or second options and considers that the steps taken in respect of the third option were inadequate.[98]

On 8 April 2014 the Court of Justice of the EU released judgment in cases *Digital Rights Ireland and Seitlinger and Others*[99] where the court declared the Data Retention Directive invalid as it entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary. The court found the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data because by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality. Therefore, the ECtHR discovered that the directive did not ensure the controlled compliance required by the Charter of Fundamental Rights of the EU European Union.

After the examination of case law of the ECtHR and the Court of Justice of the EU, it become clear that EU courts give in balancing national security with the right to privacy an advantage to human rights with requirements of proportionality, legitimacy and necessity for restrictions to be applied.

Regarding to the transparency and accountability of surveillance activities, the ECtHR ruled in *R (B.Mohamed) v Secretary of State for foreign and Commonwealth Affairs*[100] case where the Divisional Court ordered disclosure of documents by the UK government concerning details of torture on the claimant which were held by US government subject to public interest certificates which the UK government was asked to clarify despite of the US government statement that disclosure would prejudice intelligence relations between the US and the UK. The freedom of information was measured against national security interests in *Youth Initiative For Human Rights v. Serbia*[101] where the ECtHR concluded that the intelligence agency obliged to provide with certain information concerning electronic surveillance even if intelligence agency eventually responded that it did not hold that information, but that

[98]D.Voorhoof. European Court of Human Rights. Case of Peck v. United Kingdom. 2003. - http://merlin.obs.coe.int/iris/2003/6/article2.en.html.
[99]ECJ *Digital Rights Ireland and Seitlinger and Others*, C-293/12 and C-594/12, 8 April 2014.
[100]Decision of England and Wales High Court (Administrative Court) nr. CO/4241/2008 *Mohamed, R v Secretary of State for Foreign & Commonwealth Affairs*, 21 August 2008. - http://www.bailii.org/ew/cases/EWHC/Admin/2008/2048.html.
[101]ECtHR *Youth Initiative For Human Rights v. Serbia*, 48135/06, para 25, 25 June 2013.

response was unpersuasive in ECtHR has also held that when a non-governmental organisation is involved in matters of public interest, such as the present applicant, it is exercising a role as a public watchdog of similar importance to that of the press.

In 2003 the ECtHR ruled[102] that CCTV coverage of a man attempting suicide in a public place, which was shown on UK TV, was a breach of his article 8 right to privacy. In 2008 case *S. And Marper v UK*[103] the Court ruled that the blanket and indiscriminate retention of more than 857,000 records of those not convicted or charged without regard to the time limits, seriousness or age breached article 8 of ECHR. These both cases prove that the ECtHR applies the balance for the competing rights consistently which maintains the legal certainty and uphold the rule of law.

Through these examples it became evident that, in the balance for the freedom of information versus national security interests, the ECtHR continue with the approach that national security interests can be considered as an appropriate restriction to the human right only in those cases where interference with human rights was justified by passing a «triple» control test of necessity, legitimacy and proportionality by means of lawful limitations.

1.Hate speech and war propaganda regulation

The ICCPR Article 19 does not protect speech inciting hatred, violence, and discrimination, and by support of Article 20 (1) and (2) of the ICCPR, the UN Human Rights Committee stresses that "acts addressed in Article 20 of the ICCPR, are of such an extreme nature that they are subject to restriction pursuant to the Article 20 (3)[104]." But the fine line between those expressions without any seriousness set out in Article 20 (3) [105] to the acts with systematic intentions to impose threat to the State sovereignty has been noticed.

Also, the prohibition of the "propaganda of war" under the Article 20 (1) has been addressed by the UN Human Rights Committee with "any propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law", but this provision does not prohibit advocacy of the

[102] ECtHR *Peck v UK,* 44647/98, para 105.
[103] ECtHR *S. And Marper v UK,* 30562/04 and 30566/04.
[104]General Comment No 34 on freedom of opinion and expression 2011. UN Human Rights Committee. CCPR/C/GC/34, para 52. -http://www.ohchr.org/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf (14.02.3016).
[105]*Ibid*, para.54.

sovereign right of self-defence or the right of peoples to self-determination and independence in accordance with the Charter of the United Nations[106].

2.Restrictions on anonymity and encryption

In an age of pervasive online surveillance, questions of anonymity and encryption closely relate to the free flow of information, privacy and national security that are not prescribed in any international human rights instrument. Nevertheless, the anonymity and encryption must be objects of the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds; and must conform to the strict tests of necessity and proportionality.

In fact, that anonymity has been as a safeguard and advancer to privacy, free expression, political accountability, and public participation in debatesThere are very few States that provide general protection in law for anonymous expression. However, although a number of States exert significant pressure against anonymity offline and online, there are several States'judiciaries who have protected anonymity, at least in limited instances: in 2014 the Supreme Court of Canada annulled the warrantless acquisition of an anonymous online user identity[107].

An extensive number of laws in countries around the world promote the effective use of both encryption and anonymity tools. Among them are Brazil with the Marco Civil da Internet Law (2014), Austria with the E-Commerce Act and Telecommunication Act, and Greece, Germany, Ireland, Norway, Sweden, and Slovakia, as well as the United States of America, encourage the use of encryption.[108]

Nonetheless, on the UN level States are urged to provide alternative recourses and other less intrusive means than disproportionate restrictions to freedom of information and privacy by the means of prohibition of anonymity and encryption. It is left up to States by which means to achieve solutions in a dilemma when their obligation to protect freedom of expression is in conflict with their obligations to prevent violations of the right to life or bodily integrity, which are put at risk by terrorism and other criminal behaviour. So far, the requests the

[106]General Comment No 11 on prohibition of propaganda for war and inciting national racial or religious hatred 1983, para. 2.
[107]Supreme Court of Canada, *R.* v. *Spencer*, SCC 43, 2014, 13.06.2014.
[108]D. Kaye. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. A/HRC/29/32. 22 May 2015, para. 38.

disclosure of encrypted information through judicial warrants, by demonstration that general limitations on the security provided by encryption are necessary and proportionate, by showing publicly and transparently that other less intrusive means are unavailable, and that only backdoors would achieve the legitimate aim.[109] The anti-anonymity laws were declared as unconstitutional by the Constitutional Court of the Republic of Korea[110] Both, the ECHR and the Court of the United States protect the right to anonymous expression.[111]

On the other hand, there are numerous national regulations that prohibit anonymous speech online. Brazil, the Bolivarian Republic of Venezuela, Vietnam,[112] the Islamic Republic of Iran, Ecuador,[113] and the Russian Federation published separate regulations that would require users to provide identification to connect to networks[114]. These governments around the globe are working to restrict methods of anonymity and are seeking to undermine these obstacles to surveillance, potentially making the internet less secure for everyone.[115]

4. Triangular perspective

For the purpose of the achieving the aim of the thesis and to introduce the considerable solutions in the dichotomy between judicial and political powers regarding the implementation of human rights online, the thesis proposes the fresh view of seeing the problem as a complex concept of the interrelationship of all three aspects applicable in cyber matters. The view deserves attention as a three-dimensional paradigm that reflects emerging legal matters of electronic data processing and represents reality in the most adequate way. The controversy between State actors of internet society, as to the question of whether it is possible to continue the application of the balance model according to the existing universal treaties in the light of changed national security needs, and the rapid development of information technology usage among individuals, is grounded on the three demands: the right

[109] *Ibid*, para. 43.
[110] Decision 2010 Hun-Ma 47, 252 (consolidated) announced 28 August 2012. Cited in: David Kaye. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. A/HRC/29/32. 22 May 2015, para. 47.
[111] US Supreme Court, *McIntyre* v. *Ohio Elections Commission*, 1995, pp 342 and 343.
[112] Freedom House. Vietnam: freedom of the press. -https://freedomhouse.org/report/freedom-press/2015/Vietnam, 2015.
[113] S.Kelly, M.Earp, L.Reed, A.Shahbaz, M. Truong. Freedom on the Net 2015. Privatizing Censorship, Eroding Privacy. Available: https://freedomhouse.org/report/freedom-net-2015/freedom-net-2015-privatizing-censorship-eroding-privacy.
[114] Human Rights Watch Submission: World Development Report on Internet for Development. Human Rights Watch. - https://www.hrw.org/news/2015/08/26/human-rights-watch-submission-world-development-report-internet-development, 26.08.2015.
[115] Ecuador.Freedom on the Net 2014. Organic Law on Communications 2013.Available: https://freedomhouse.org/sites/default/files/resources/Ecuador.pdf.

to privacy, the freedom of information, and national security. So far, the related matters have been seen mainly through a two-sided approach, which may not be sufficient. However it is not wrong to continue with the same approach has been deployed during the last decades, but it may leave essential elements of the reality unaddressed. The thesis has chosen the three-dimensional approach and its argumentation is based on this point of view. The three corners are not random, rather they are identified as they interrelate to each other.

The legality of this view is based on the case-law of the ECtHR. For instance, in *Hatton v United Kingdom*, the ECtHR underlined that whatever analytical approach is adopted, regard must be had to the fair balance that had to be struck between the competing interests of the individuals and the community as a whole.

In 2015, the UN Special Rapporteur admitted the worrying trend lines regarding security, freedom of information and privacy online while states fail to provide public justification to support restrictions.[116] Rapporteur reminded to States to read the permissible limitations on the rights strictly[117] according to all accepted rules of derogation to apply. This view is supported by the case *The Sunday Times* v. *United Kingdom*[118], where the ECtHR confirmed that the restriction must be something more than "useful," "reasonable" or "desirable".

According to the data privacy laws research in 2012, it has been revealed that the standard established by the European Union regulations and complementing case-law, has influenced the majority of the world's countries. Because of the reason, that it originates from the legal standards established in the UDHR and in the ICCPR. Both follow similar approach to the interrelation between human rights the same logic of subordination for rights and relevant restrictions, legally binding on all UN Member States.

III Midway conclusions

The first chapter of thesis indicated what is the minimum scope of protection for international human rights, specifically for privacy and freedom of information in regards to national security. The nature of the right to privacy in online protection covers the protection of individuals against any attacks on honour and reputation, the use of a person´s name, identity, or likeness, without being spied upon. Protected is any activity online concerning an

[116]D. Kaye, para 36.
[117]D.Kaye, para 29.
[118]ECtHR *The Sunday Times* v. *United Kingdom*, 538/74, 26 April 1979, para. 59.

individual´s data transmission via Internet is included to the protection of the private sphere. Freedom of information appears to be information to br protected regards to all kinds and sorts of expression and the means of their dissemination, whether spoken, written and sign language and non-verbal expression, shared including in the Internet. And the national security concept entails protection of State´s national values, its normal functioning, interests and goals, means and methods preventing and reflecting internal and external threats. The legal expectations contained in international human rights treaties for States to be respected, based on the case-law of the the Court of Justice and of the EU ECtHR, that considered values should be treated with equal respect and that national authorities have to follow the requirement of prevalation of rights over exceptions provisioned to balancing when two protected rights.

B Current State Practice

I Relevant State Practice

1. The United States

1) Regulation

The private life protection is enshrined in Article 11 (1) of the American Convention on Human Rights (hereinafter ACHR) which is similar to the ICCPR in content. Article 13 (1) guarantees the right to freedom of thought and expression, including freedom of information[119] and is also similar to the ICCPR.[120]

Comparing to the Article 10 of the ECHR to the Article 32 of the Arab Charter, Article 9 of the African Charter on Human and Peoples´ Rights (hereinafter ACHPR), the Article 13 of ACHR follows the similar ideology for the liberties that are objects to the limitations to what is allowed within the law and are according to the "collective security" or "common interest" protection. The "law" has been interpreted globally as being consistent with international law, specifically the aim and purpose of the UN Charter, so "international human rights standards must always prevail over contradictory national law"[121]. Thus, the common nominators can be drawn from the American and European Constitutions as both stand for the protection of internationally recognised human rights and give priority to international human rights even in cases where national law appear with contradiction.

The US Consitution the Fourth Amendment protects all Americans against unreasonable searches by the government.[122] Right after 9/11 in 2001, the US signed the Patriot Act that bypasses the Foreign Intelligence Surveillance Court (hereinafter FISA Court) and allows direct spying through a new NSA electronic surveillance program.[123] The FBI collected Americans' communications under Section 702 of the Foreign Intelligence Surveillance Act (hereinafter FISA)[124] without a warrant or judicial oversight. Currently, according to the Bill

[119] Peter Malanczuk, para. 57.
[120] L.Doswald-Beck, p.401.
[121] L.Doswald-Beck, p.403.
[122]S. Bradbury. Balancing Privacy and Security, p 1. -http://www.harvard-jlpp.com/wp-content/uploads/2015/02/Bradbury_Final.pdf (30.03.2016).
[123]Working Draft. Office of the Inspector General. ST-09-0002.-http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection (24.03.2016).
[124]Electronic Privacy Information Center. Foreign Intelligence Surveillance Act (FISA). https://epic.org/privacy/terrorism/fisa/.

of Rights Defense Committee, three states (Alaska, Hawaii, and Vermont) and 149 cities, towns and counties have passed resolutions protesting provisions of the Patriot Act[125].

It is noteworthy, that before the 9/11 terrorist attacks, the United States courts, since 1971, that the threat level is not sufficient to impose restrictions to the civil liberties. Therefore, there was not such a threat to the national security that would justify an infringement of the core values of society. For example, in the *New York Times Co. v. United States*[126] the court ruled that, in attempting to suppress the Pentagon Papers, the government failed to meet the «*heavy burden of showing justification for the imposition of prior judicial restraint*». So, before the terrorist attacks to the US, courts as well complied with the international human rights standards. The 9/11 terrorist attacks caused a crucial shift in the balance for privacy, freedom of information, and national security in the US as these accidents created the greatest distinction between the EU and US approach caught through idea of the "exception".[127] As a result, during Busch administration initiated "war on terror", the US courts case-law started to decide in favour of national security interests causing the shift in the balance which was is seen as evasion and erosion of the rule of law.[128]

Among other provisions, the record search provision made it possible for the FBI to secure client records without judicial oversight, and without prior notification of the person under surveillance. The accountability and oversight were not prioritised.[129] Thus, the US judicial concept of balance moved closely to the legislative one to the completely opposite side from the previous position and started to contradict against the judicial balance established by the case-law in the ECtHR.

2) Practice

The jurisprudence of the US Supreme Court has erected strong defences of the freedom of speech in America. In *New York Times Co v United States,*[130] for example, the Supreme Court rejected the claim of the US government that it was entitled to censure the publication by the

[125] The Patriot Act: What Is the Proper Balance Between National Security and Individual Rights?. Available: http://www.crf-usa.org/america-responds-to-terrorism/the-patriot-act.html.
[126] US Supreme Court, *New York Times Co. v. United States*, no. 403 U.S. 713, 30 June 1971, p. 230.
[127] C. Murphy. EU Counter-Terrorism. Pre-Emption and the Rule of Law. Oxford and Portland, Oregon: 2012, p. 230.
[128] C. Murphy. EU Counter-Terrorism Law: Pre-Emption and the Rule of Law. Oxford: Hart Publishing 2012, p 236.
[129] D. McLeod, D. Shah. News Frames and National Security: Covering Big Brother. New York: Cambridge University Press 2015, pp 1, 2.
[130] ECtHR *The Sunday Times* v. *United Kingdom*, 538/74, 26 April 1979, para. 59.

New York Times and Washington Post of the then-classified Pentagon Papers that had been prepared and compiled by government officials responsible for conducting the Vietnam War. The Supreme Court upheld the right of the editors to publish the materials on the basis of the constitutional guarantee of the freedom to speak and to publish as laid down in the First Amendment. It dismissed the claim of the Nixon administration to secure confidentiality of the information and denied that the government was entitled to a prior restraint order prohibiting publication in the first place.[131]

2. The United Kingdom

1) Regulation

The contending situation within the UK escalates by the political, economical and legal tension arising between UK and EU. The British cases of the Investigatory Powers Tribunal (hereinafter IPT) are brought before the ECtHR, in *Liberty & Others v. the Security Service, SIS, GCHQ* and *Big Brother Watch v. UK* that concerns bulk data collection, data sharing, and Britain's existing legislation relating to human rights,[132] where the ECtHR is called upon to determine the issue about collection of data and provide the final word on the matter. The rulings of the ECtHR lay the dilemma before the UK as the upcoming decisions of the ECtHR will be the outcomes of the crosscontinental battle between the UK´s and EU´s legislative and executive powers with judicial ones and may cause far-reaching consequences for the future of the UK in the EU. Therefore, given its role to developments in the UK and its relations with its allies and partners are of continuing interest of the British government.

In November 2014 the premise was affirmed by the UK Home Secretary Theresa May who addressed her strong view to the courts that the provisions of a Counter-Terrorism and Security Bill are compatible with the ECHR and should be implemented.[133] On the 5th December 2014 the *IPT in Liberty & Others v. the Security Service, SIS, GCHQ* has ruled that Britain's legal regime governing mass surveillance of the internet by intelligence agencies does not violate human rights.[134] In February 2015 for the first time the IPT found that

[131] P. Malanczuk, p. 111.
[132] GCHQ does not breach human rights, judges rule. BBC News 5.12.2014. - http://www.bbc.co.uk/news/uk-30345801.
[133] Home Secretary Theresa May on counter-terrorism, 24 November 2014, Royal United Services Institute, https://www.gov.uk/government/speeches/home-secretary-theresa-mayon-counter-terrorism.
[134] GCHQ does not breach human rights, judges rule. BBC News 5.12.2014. - http://www.bbc.co.uk/news/uk-30345801.

GCHQ's access to information obtained by the US National Security Agency's PRISM and Upstream programmes was illegal.[135]

In the UK, regulation on surveillance exists in the Regulation of Investigatory Powers Act 2000 which deals with directed surveillance and intrusive surveillance which is a) carried out in relation to anything taking place on any residential premises or in a private vehicle, and b) involves the presence of an individual on the premises (such as a paid informer or someone who is concealed) or is carried out by means of a surveillance device. The Act is designed to ensure that practice in this area is brought into line with the ECHR requiring that the different kinds of surveillance are authorised in advance, the authorisation in some cases now requiring judicial approval. It still has been argued[136] that, the UK lacks an impartial safeguards system to ensure against the abuse of such powers.

In 12 February 2015, the Parliament adopted the new Counter-Terrorism and Security Act, intended to give Britain some of the "toughest powers in the world"[137] against terrorism. In 17 July 2015 the High Court of UK ruled that the Data Retention and Investigatory Powers Bill (DRIPA), a year after it was amended, is unlawful because the law fails to provide the "clear and precise rules" and, therefore, its sections 1 and 2 breach Articles 7 and 8 of the EU Charter of Fundamental Rights. Right before amendment of the DRIPA, the Court of Justice of the European Union[138] decided that Data Retention Directive is invalid because of unspecific security measures enabled by this. DRIPA was designed to give GCHQ and other public intelligence authorities the power to gather and retain information on phones calls, text messages and online communications, and force telecommunications companies to retain data for 12 months.[139]

Members of Parliament David Davis and Tom Watson challenged existing DRIPA regulation in High Court to be rewritten with requirement of judicial or independent approval before

[135] D. Davis. David Davis: Parliament insulted our democracy with surveillance bill. 2407.15. - http://www.wired.co.uk/news/archive/2015-07/24/david-davis-dripa-judicial-review (22.03.2016).
[136] A. Fishman, G. Greenwald. Spies Hacked Computers Thanks to Sweeping Secret Warrants, Aggressively Stretching U.K. Law. -The Intercept_. - https://firstlook.org/theintercept/2015/06/22/gchq-reverse-engineering-warrants/, 22.06.2015.
[137] M. Holehouse. Counter-terrorism Bill: What it contains. -The Telegraph 26.11.2014.- http://www.telegraph.co.uk/news/worldnews/islamic-state/11254950/Counter-terrorism-Bill-What-itcontains.html.
[138] The Court of Justice declares the Data Retention Directive to be invalid. Court of Justice of the European Union, Judgment in Joined Cases no. C-293/12 and C-594/12, 8 April 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.
[139] L. Clark. UK mass surveillance laws are unlawful, it's official. -http://www.wired.co.uk/news/archive/2015-07/17/uk-surveillance-laws-are-unlawful, 17.07.15.

accessing people's data. The High Court ruled that DRIPA fails to demand a warrant from a court or independent body. In the space of June and July 2015 two reports reflecting the new consensus amongst experts in the Anderson[140] and RUSI reports[141] came to conclusion that intelligence agencies be required to attain judicial sign off - rather than ministerial - for interception warrants.

2) Practice

The UK laws personal data have existed since 1984 and superseded by the Data Protection Act 1998. Before these regulations paper records were held by employers on employees had been stoutly resisted in spite of notorious episodes concerning abuses by self-styled private vetting agencies.[142] In March 2009 the Information Commissioner issued a press release with details of a database held by a consulting company with details of 3,213 construction workers. Data had been sold to over forty construction companies to vet individuals for employment.[143] The possibilities involving unregulated use of genetic information amount to the implications of commercial patenting of such information are startling. The Department of Health sells information on its database that records patient reaction to pharmaceuticals.[144] In 2001 the Metropolitan Police refused to destroy 3.500 DNA profiles taken from people questioned but subsequently ruled out of police investigations.[145]

In *R v Home Secretary* case (1987) was ruled that Interception of Communications Act 1985 provides a number of new safeguards to restrain any possible misuse of the new statutory procedures, addressing concerns that the practice of telephone tapping had been abused previously. In the case *Halford v United Kingdom*[146] of the ECtHR held that the UK was in breach of art 8 for failing to regulate the interception of communications of employers. In response to new technology and new means of communication. In particular, as was held in *R*

[140] D. Anderson. A Question of Trust. Report of the Investigatory Powers Review 2014.- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf (30.01.2016).
[141] RUSI. A Democratic Licence to Operate Report of the Independent Surveillance Review. London, Brussels: Royal United Services Institute for Defence and Security Studies 2015.- https://www.rusi.org/downloads/assets/ISR-Report-press.pdf.
[142] What price privacy now?, The first six months progress in halting the unlawful trade in confidential personal information, 13 December 2006, https://ico.org.uk/media/about-the-ico/documents/1042392/what-price-privacy-now.pdf.
[143] *Ibid*.
[144] *R. v. Department of Health, Ex Parte Source Informatics Ltd*., 2000, http://medlaw.oxfordjournals.org/content/8/1/115.full.pdf.
[145] The Criminal Justice and Police Act 2001, allowed for the retention of DNA and finger-print samples even where there was an acquittal or decision not to prosecute.
[146] ECtHR *Halford v United Kingdom*, 1997 24 EHRR 523.

v Effic[147] case that the 1985 Act did not apply to the use of cordless phones. These issues have been addressed in the RIPA 2000 Part I, but after its inactment were expressed doubts whether new provisions are sufficiently comprehensive.[148] So, it becomes obvious that the practice of interceptive means to the communications via electronic devises has been widely used by the UK, but the case-law of the ECtHR fulfilled commitment to maintain the human rights in compliance with the main UN international treaty bodies.

While the UK is adopting tough legislation, asking for state effectiveness in protecting its critical infrastructure is justified. Governments have not always taken effective remedies to protect its important public service means. At the same time major responsibility for securing informational infrastructure lies with the private sector which reduces the level of infrastructure protection. For example, US public information systems are not comprehensively protected due to outdated software used in computers and the lack of demand for legislation to renew in a mandatory way effective protective software to grant protection against known viruses. Also, a low level in staff education related to protection of information systems was found.

2. France

1) Regulation

The January 2015 attacks in Paris have highlighted the threat of domestic terrorism in Europe and put the continent on high alert. Europol announced on January 13th that an estimated 5,000 European citizens have joined the ongoing armed conflict in Syria and pose a direct threat to their home countries upon their return. Some of the recently reported cases in France may cross the high threshold of expression that can legitimately be prosecuted.

A wave of cases opened by the French judiciary over the past years against people for allegedly “glorifying terrorism,” some of whom have already been summarily sentenced to imprisonment, shows the contradictions in France’s approach to the right to express opinions that offend, shock, or disturb. In 21 January 2015 hackers attacked website of the France´s biggest newspaper Le Monde and France's measures to prevent people from defending terrorism have gone overboard.

[147] ECtHR *R v Effic*, 1995 1 AC 309.
[148] Y. Akdeniz, N. Taylor, C. Walker. BigBrother.gov.uk: State surveillance in the age of information and rights. 2001. p 2. - http://www.leeds.ac.uk/law/staff/law6cw/clrrip06.pdf.

France has ratified all the main international legal instruments on human rights in which freedom of opinion and expression is enshrined. Freedom of expression is expressly recognised in article 19 of the UDHR and in articles 19 and 20 of the ICCPR.

France supports the mandate of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, established in 1993. A number of resolutions on freedom of opinion and expression, co-sponsored by France, have been adopted by first the Human Rights Commission and then the Human Rights Council over the years, reaffirming the principle that freedom of expression is an essential freedom in a State under the rule of law.

France also supports freedom of expression through the Council of Europe. France is subject to the jurisdiction of the ECtHR as regards the implementation of article 10 of the European Convention on Human Rights in which freedom of expression is enshrined. The Committee of Ministers of the Council of Europe has also adopted the Guidelines on protecting freedom of expression and information in times of crisis.

The arrests and prosecutions are the first to be carried out under the November 2014 counterterrorism law. They are based on a criminal code article under which “inciting” or “defending” terrorism carries a sentence of up to five years in prison and a fine of EUR 45,000, and up to seven years and a EUR 100,000 fine if it involved posting something online.[149] While “incitement” and “defence of terrorism” were already offences in France, the November 2014 law moved them from the press law to the criminal code. This means the process can be fast-tracked by the authorities.

France is committed to defending freedom of expression, including on the Internet. The Internet can be used, however, as a vehicle for the propaganda of hate and for material potentially prejudicial to public morals and health or to the security of the State. There is a risk that notions such as "defence of terrorism” will be used to criminalize statements made without the necessary element of intent and the direct and immediate likelihood that they would prompt such violence. French law allows for people to be sentenced to up to five years in prison if they commit the broadly worded offenses of “inciting” or “glorifying” terrorism.

[149] France faces ‘litmus test’ for freedom of expression as dozens arrested in wake of attacks. - https://www.amnesty.org/en/latest/news/2015/01/france-faces-litmus-test-freedom-expression-dozens-arrested-wake-attacks/, 16.01.2015.

As a reflection to France´s national security situation, in November 2014 France adopted the new counterterrorism law which legalised electronic surveillance by public bodies and increased the sentence to seven years if either offence is committed online. In January 2015 France doubled down on an existing law that allows the shutdown of websites deemed to be «sympathizing with terror».[150]

The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the OSCE Representative on Freedom of the Media have incorporated this issue into their investigations and recommendations. These two experts, alongside their counterparts at the Organisation of American States (OEA) and the African Commission on Human and People's Rights, issued a joint declaration in March 2010 identifying ten key challenges to freedom of expression worldwide, including efforts by some governments to control or limit the Internet.

2) Practice

France is exercising the Internet content control practices. In *Yahoo* case in France illustrates a clash of legal cultures regarding Internet content control among democratic societies. In May 2000, the Paris Tribunal de grande made an interim ruling ordering Yahoo to take measures to make it impossible for its disputed sites and services to be accessed through Yahoo.com by a surfer calling from France. Yahoo's California-based company provided information services on its US-based website which permitted traffic of material glorifying Nazism. In the US, this is protected by the First Amendment. In France, it is barred by French law and punishable under the French Penal Code. The Paris Tribunal based its ruling on the assumption, following technical expert advice, that effective filtering methods were available to Yahoo making it possible to block access to the Nazi material by French residents without removing it more generally (also for US citizens, for example). In addition to the injunction and the risk of financial penalties in the civil action, Yahoo as a company and its CEO were confronted with criminal charges, but were acquitted in a French court decision that was finally upheld on appeal in 2005. Yahoo responded to the injunction issued in the civil action by seeking a declaratory judgment in US courts that the French orders were unenforceable in the US. While the first ruling by a Californian District Judge agreed that the French orders violated public policy as laid down in the First Amendment and were therefore unenforceable

[150] A. Masi. France's Online War on Terror Sympathizers and Extremists Has A New Cyber Security Cell. - International Business Times. -http://www.ibtimes.com/frances-online-war-terror-sympathizers-extremists-has-new-cyber-securitycell-1786662, 17.01.2015.

by a US court, in the end Ninth Circuit dismissed the *Yahoo* case on the basis of six strongly divided opinions[151].

4. The Russian Federation

1) Regulation

The compliance of the Russian Federation legislation to the standards in international human rights treaties has been question of divergent sides. From the one side, the Russian Federation strengthened its commitment to the protection of personal data by ratification the ECHR on 5 May 1998 Russia[152] and the Council of Europe Convention on 15 May 2013. The Russian Federation also signed on 13 March 2006 the additional protocol to Coe regarding supervisory authorities and transborder data flow.[153] The Article 24 of the Russian Constitution stipulates that it is not permissible to collect, store, use or disseminate information about a person's private life without his/her consent. State and municipal authorities must ensure that any person has access to documents and materials affecting his rights and freedoms, except where the law provides otherwise. Article 24, accompanied by the relevant federal laws, provides additional safeguards for the data protection pursuant to the Article 8 of the CoE. Corresponding national laws, such as the Communications Act of 7 July 2003 (no. 126-FZ) guarantees the privacy of postal, telegraphic and other forms of communication transmitted by means of telecommunications networks or mail services. Restrictions on the privacy of communications are permissible only in cases specified in federal laws (section 63(1)). The interception of communications is subject to prior judicial authorisation, except in cases specified in federal laws. Moreover, the Article 55 (3) of the Russian Constitution allows measures to interfere into private communications should be granted by the judicial warrants. All human rights limitations should be interpreted restrictively and applied only according to the provisions prescribed by law.[154]

---

[151] United States Court of Appeals, *Yahoo! Inc v La Ligue Contre le Racisme et l'Antisemitisme*, C-00-21275JF, 2006.

[152] ECtHR. Russia. Press Country Profile. Available: http://www.echr.coe.int/Documents/CP_Russia_ENG.pdf.

[153] The Joint Supervisory Body of EUROPOL. Opinion 08/44 of the JSB in respect to the data protection level in the Russian Federation. - http://www.europoljsb.europa.eu/media/213359/0844%20jsb%20europol%20opinion%20on%20dp%20level%20in%20russian%20federation.en.pdf, 8.10.2008.

[154] Постоянное представительство Российской Федерации в ООН и других международных организациях в Женеве. нформация резолюции , принятой Генеральной Ассамблеей 18 декабря 2013 68/167 . Право на неприкосновенность частной жизни в цифровую эпоху. 9 апреля 2014 г., http://www.ohchr.org/Documents/Issues/Privacy/Russia.pdf.

2) Practice

From the pratical side, the ECtHR revealed in the most recent judgment, *Zakharov v. Russia*[155], on the proper limits of communications surveillance powers under Russian law that Russia's SORM system, which is present in Russia and in Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan[156], is not consistent with the requirements of Article 8 of the ECHR. The ECHR noted in its final verdict under following reasons:

A) "Threat to national security" in the Russian law does not explain how such a broadly worded term should be interpreted in legal practice, and thus it gives law enforcement agencies too broad discretion determine what events or activities pose a threat to the above, and whether this threat is serious enough to justify the interception of telephone negotiations.

B) Russian legislation does not clearly determine the situations in which wiretapping should be discontinued. The requirement for immediate cessation of listening when the need for this measure disappears, is found only in the Article 186 of Criminal Procedure Code, but not in the law on Federal Law on Investigative activity. As a result, wiretapping on the basis of the law of Federal Act on Investigative Activity (in particular, connection with obtaining information about events or actions that threaten government, military, economic, or environmental information Russian Security) is carried out without sufficient guarantees Port of abuse.

C) Russian law allows to be stored for six months all materials collected as a result of wiretapping. It does not contain requirements for the immediate destruction of the materials that are obviously not associated with the listening purposes. In addition, the legislation does not stipulate in what situations the materials that have been used in a criminal trial, must be destroyed after the termination of this process, and in which situations they can continue to be stored.

D) The procedure for issuing permits for wiretapping does not provide sufficient guarantees that listening will only be allowed in cases where it is necessary and justified. In particular, in spite of the instructions of the Constitutional court, Russian courts do not check whether there are grounds to suspect a person of listening to telephone conversations whose intercede law authorities of involvement in the crime or acts endangering national security of Russian Federation. The Russian courts also do not evaluate the validity and the need to listen. In particular, to requests for hearing telephone conversations are often attached for evidence

[155] ECtHR. *Roman Zakharov v. Russia*. Application no. 47143/06, 4 December 2015.
[156] Private Interests: Monitoring Central Asia. Special Report, p 18. - https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf, 11.2014.

grounds for listening, and judges do not require the submission of such materials. Normally to obtain judicial authorization to audition law enforcement bodies is sufficient to refer to the availability of information on crime or actions that threaten the national security of the Russian Federation.

In addition, the Federal Act on Investigative Activity does not contain any requirements for the content of any application for listening to telephone and other conversations or judicial permission for this audition. As a result, courts sometimes issue permits for listening to all mobile phone calls in the area of fulfillment crime, without specifying a particular person or phone number, or permission to audition without specifying the period of validity. The the Federal Act on Investigative Activity lets you listen to telephone and other negotiations for 48 hours without prior judicial authorization in cases that are not urgent. This procedure does not provide sufficient procedural safeguards that it will only be used in cases where it is really justified.

Finally, the ECHR came to the conclusion that the technical equipment to ensure functions of search operations in the telecommunication networks (SORM - 2) gives law enforcement agencies the technical ability to listen Mobile telephone conversations without first obtaining a court authorization, ie bypassing the legal procedures. Although, abuses are possible with any system of secret surveillance organization, their probability is particularly high in such a system in Russia, where the law enforcement agencies are using technical means of direct access to all mobile telephone calls and required to present the resolution to the audition or mobile operators or anyone else. With this system, the need for effective procedural safeguards against abuse is particularly high.

E) Supervision over the legality of covert operative-search activities does not meet the requirements of the ECHR on the independence of the supervising authority, sufficient authority to carry out effective supervision and transparency public control. Firstly, the prohibition on the registration of information about controlled subscribers and other information relating to the interception mobile telephone conversations is making it impossible to identify cases of illegal wiretapping processed without court permits. Secondly, supervision is operated by the General Prosecutor and authorized by him/her prosecutors. Considering the procedure for appointing prosecutors, the ECHR experienced doubts as to their independence from the executive power. Moreover, the fact that the prosecutor's office combines the functions of the criminal prosecution and, simultaneously, of the legality plays supervision telephone and other conversations, gives reason to doubt in its independence.

Thirdly, the prosecutor's office powers of supervision over the legality of auditions is limited: for example, the subject of prosecutor's supervision does not include information on tactics, methods and means of implementation of the activities of the organs of federal security services. In addition, the Russian legislation does not contain demands the immediate destruction of the materials that have been qualified as a prosecutor resulting from illegal wiretapping. Fourth, the results of prosecutorial supervision are not published or made public in any otherwise. Finally, the Russian Government has not provided any prosecutorial decisions which ruled to stop the violation of the rights or take measures to restore them and bring the perpetrators to justice officials do not proving thus the effectiveness of prosecutorial supervision in practice.

F) While the ECHR examined the effectiveness of the means of appeal to permit wiretapping by phone or other communications, it detected that the effectiveness of these means of appeal is undermined by the fact that they are only available to those who can provide proof of listening to their phone negotiations. In the absence of listening of telephone notification system negotiation or an effective opportunity to seek information about the audition, receive such proof is almost impossible. Thus, a person who suspects that his telephone or other communications are monitored, there are no effective means of appeal - one of the most important guarantees against abusive uses of covert surveillance techniques. Based on above, the ECHR held that Russian legislation does not meet the criteria of "quality of the law " and not able to restrict the use of covert surveillance techniques only to those cases where it is "necessary in a democratic society".

The Russian Constitution stipulates that it is not permissible to collect, store, use or disseminate information about a person’s private life without his/her consent. State and municipal authorities must ensure that any person has access to documents and materials affecting his rights and freedoms, except where the law provides otherwise (Article 24).

The Communications Act of 7 July 2003 (no. 126-FZ) guarantees the privacy of postal, telegraphic and other forms of communication transmitted by means of telecommunications networks or mail services. Restrictions on the privacy of communications are permissible only in cases specified in federal laws (section 63(1)). The interception of communications is subject to prior judicial authorisation, except in cases specified in federal laws (section 63(3)). Thus, Russian law prohibited maintaining records of interception.

The ECHR noted that supervision of interception by judges and prosecutors was limited and not open to public scrutiny. The absence of a requirement to notify the subject when surveillance had ceased further undermined the effectiveness of any available remedies. Consequently, Russia's SORM system was found violating the right to privacy enshrined in Article 8 of the ECHR.

Moreover, the Court of Justice of the European Union (hereinafter CJEU) held on the retention of communications data after the uncertainty that has followed invalidation of the EU Data Retention Directive, in the *Digital Rights Ireland*[157] case, that Russian law was seen to give judges too much discretion to decide whether data should be stored after the conclusion of criminal proceedings.

5. China

1) Regulation

At the Spring 2016, China is not bound to the specific provisions of the ICCPR, but as a signatory State, has the obligation to act in good faith and not defeat the purpose of the ICCPR according to the customary international law.[158] On the international community level, China continues to insist that human rights should be implemented according to a country's national conditions.[159]

As a result of Chinese specific view regards to the international law obligations, the implementation of data protection standards in China proceeds with Chinese characteristics. Currently, data protection and privacy regulations in online context might be considered as the most extensive and restrictive in the world.[160] The Chinese concept of cybersecurity involves four main principles: security of cyberspace sovereignty, security of Internet information, security of privacy in cyberspace, and security of information technology.[161] From these four perspectives the national legislation on data protection within context of

[157]CJEU. *Digital Rights Ireland Ltd v Ireland*. Joined Cases C-293/12 and C-594/12. 8 Apri 2014, paras. 255-56.
[158]UN Treaty Bodies and China. -Human Rights and China. -http://www.hrichina.org/en/un-treaty-bodies-and-china (13.04.2016).
[159] S. Sceats, S. Breslin. China and the International Human Rights System. Chatham House. October 2012, p. 1. https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/r1012_sceatsbreslin.pdf (13.03.2016).
[160]How Censorship Works in China: A Brief Overview. -https://www.hrw.org/reports/2006/china0806/3.htm (14.03.2016).
[161]Z. Zhou. China's Draft Cybersecurity Law. The Jamestown Foundation. -http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44924&cHash=db05078399a49339345c2957196d4073#.VyUAwdR968o, 21.11.2015.

national security should be observed. In 2012, the new rules were approved to strengthen the legal basis for real-name registration by websites and service providers by Chinese public authorities. Since November 2014, the new counterterrorism law required to provide "backdoor" access and copies of encryption keys to all telecommunications companies and internet services to the government.[162] The registration of real- names is mandatory and the rules offer no protection against law enforcement requests for these records.[163]

Current developments in Chinese electronic data protection legislation are progressive. For the purpose of encountering emerging threats, in 2015, China adopted an extensive National Security Law with an expansive definition of national security.[164] According to Article 34 and 35of the China's Draft Cybersecurity Law, China ISPs are required to meet their legal obligation to protect personal information under the legality, legitimacy and necessity principles. They are also required to adopt measures necessary to keep the personal information collected strictly confidential (Article 36). An individual has the right to request the deletion of his or her personal information collected or used by the ISPs (Article 37).

Also, nobody is allowed to acquire or disclose the personal information of others in an illegal manner (Article 38). Government authorities must not disclose any personal information obtained while performing their duties (Article 39). As for censorship measures, ISPs are obligated to stop the spread of information prohibited by law (Articles 40 and 41) and to set rules for handling complaints on Internet information (Article 42). The public offices are empowered to order ISPs to block the transmission of such illegal information (Article 43). All these provisions has raised doubts among to scholars[165] that the law is not really meant to protect cyberspace privacy, rather, is intended to carry out Internet censorship under the pretext of privacy protection.

In sum, it is beneficial route for China to abstain from binding obligations under international regards to the blocking access to online material as it is subject to the highest level of scrutiny, with a burden on the government to demonstrate that censorship would effectively avert a threat of irreparable, imminent, and weighty harm, and that less extreme measures are

[162] China. Country Report. Freedom on the Net 2015. -https://freedomhouse.org/report/freedom-net/2015/china.
[163] D. O'Brien. China's name registration will only aid cybercriminals. Committee to Protect Journalists blog. - https://cpj.org/blog/2012/12/chinas-name-registration-will-aid-not-hinder-cyber.php, 28.12.2012.
[164] Chun Wong. China Adopts Sweeping National-Security Law. -The Wall Street Journal. - http://www.wsj.com/articles/china-adopts-sweeping-national-security-law-1435757589. 1.07.2015.
[165] L. Zhou. Chinese cyber regulators are getting personal.-Business Insider 4.02.2015. - http://www.businessinsider.com/chinese-cyber-regulators-are-getting-personal-2015-2?IR=T (18.04.2015).

unavailable as alternatives to protect the state interest at issue. At present, it seems apparent that China engages in no such scrutiny, and instead continues with censors an immense amount of material.

2) Practice

In 2011, China was ranked as a country with the most aggressive Internet censorship system where citizens are sentenced in prison sentences for writing about politically sensitive topics online.[166] In this regard, the UN Special Rapporteur takes the position that Internet users confidence and security on the Internet is undermined in China and in the Republic of Korea. Therefore, the free flow of information and ideas online is impeded as States and private actors have access to new technologies to monitor and collect information about individuals communications and activities.

Unfortunately, Asian region (Hong Kong, China) maintains abuse of human rights despite internationally recognized standards as there is not an obligation to abide by the laws of others. For example, China still practices its despotic politics and in order to gain a bigger stake in the Chinese market betraying the interests of its customers is inevitable.[167]

Chinese state behaviour, for example, shows an unwavering commitment to curtailing internet freedom in the name of state security. The internet restrictions documented in 2013 were faster and more nuanced than ever before.[168] They tightered controls on content, measures to deliberately slow internet traffic, and intensified harassment of dissidents, as the Chinese Communist party's propaganda and security agencies worked to eliminate any nascent political challenge,[169] leaves a growing community vulnerable to invasive rights violations.[170] Chinese manifest in the phrase "internet sovereignty," meaning the right to practice censorship within Chinese borders.[171] Violations of users rights are proven by governmental

[166]T. Lum, P. Figliola, M. Weed. China, Internet Freedom, and U.S. Policy. -Congressional Research Service, p 1. -https://www.fas.org/sgp/crs/row/R42601.pdf, 13.07.2012.
[167] Human Rights Watch, China, "Race to the Bottom" Corporate Complicity in Chinese Internet Censorship", August 2006, p 117, http://www.hrw.org/reports/2006/china0806/china0806webwcover.pdf.
[168] China. Freedom of the Net. 2013, p 3. - https://freedomhouse.org/sites/default/files/resources/FOTN%202013_China.pdf (16.03.2016).
[169] *Ibid*, p 3.
[170] *Ibid*, p 23.
[171] *Ibid*, p 13.

activity to sentence people in a closed trial to eight years in jail for discussing democracy online.[172]

Despite of universal principles China concerning to the right to privacy is overseeing the fact that prior censorship in particular is severely disfavored in international law, and not permitted in many constitutional systems. Chinese regulations undercut the right to privacy of Chinese web users.[173] By requiring ISPs to maintain the capability to read the communications of individuals communicating online, and even to be able to keep records of which websites individual netizens choose to visit, the Chinese government is seriously infringing on the privacy rights of its own people.[174] Although the Chinese constitution explicitly protects the right to free expression, theright to privacy, and the right to engage in academic research, the constitution itself isnot directly enforceable, and therefore regulations that clearly violate these rights escapeany form of judicial scrutiny.[175] The overall institutional weakness and lack of independence of Chinese courts also plays a key role. Because most courts in China receive the majority of their funding from the local government,they are often unable or unwilling to deliver a verdict contrary to the local expectations, especially in politically sensitive cases. Courts are also subject to both government and Communist Party authority, and must please both masters.[176] Similarly to right to information states consider approaches related to right to privacy.

II Reasons for States Practice

This section indends to identify if any contradiction are met, what are the reasons that States used to justify practise online security measures contrary to the international treaties. In the case, when these reasons can be solved by international law measures, the thesis will consider possible recommendations on potential detailed solutions for achieve consistency and coherence of State practices for maintaining the unity and clarity of the most national regulations.

As was noticed earlier regards to the States under the focus, except for the China, there is the gap between their political order and internationally accepted standards states have been

[172] China. Freedom of the Net. 2013, p 3.
[173] China: "Race to the Bottom": Corporate Complicity in Chinese Internet Censorship. Human Rights Watch, p 22. - http://www.hrw.org/reports/2006/china0806/china0806webwcover.pdf, 08.2006.
[174] *Ibid,* p 23.
[175] *Ibid,* p 23.
[176] *Ibid,* p 23.

committed by international treaty bodies. China is appearing as an exception because China has not ratified the ICCPR nor any other international law instrument that would be applicable to the balance of privacy, freedom of information and national security. In this section reasons for this incoherence will be discussed and revealed.

One of the reasons why the balances established in the US and the EU Member States courts case-law differ substantially is that the EU States are not engaged in military action on the same scale as the US that has its corresponding legal and administrative policy developments.[177] The involvement of US entailed its effective ability to protect its nation against any threats against national security, including cyber threats. The EU as a region is not involved into military operations and therefore its case-law correspond to the needs of defence justification. By this, this reason can be solved by international law measures.

Apparently, one of the reasons that cause disharmony between judicial and political views on the balance between human rights and national security, is questionable ability of international treaties to adjust to modern-day threats to national security. Social reality changed the way that it is not compatible with the protection scope of treaty that drafters of international law treaties were not able to foresee.[178] Rapid development of computing technology has accelerated change in social behaviour and attitudes so States have considered restrictions of human rights in Internet in order to meet modern threats to national security. Individuals become more comfortable with being connected to the Internet at all times. Movement toward more natural human-computer interfaces is driven by the acceptance of wearable Internet nodes[179]. A variety of forces- personal, corporate, and economic- widened channels to the consumer technology market, so it became widely adopted and customised in society. And now constant change in technology development according to Moore´s law enables significantly more powerful devices for a more great percentage of the world population.[180] The trend addresses the growing dependency on information and communications technologies in all domains of human life[181] and is moving toward more

[177] C. Murphy. EU Counter-Terrorism Law. Pre-emption and the Rule of Law, p. 27.
[178] C. Diggelmann, M. Cleis. How the Right to Privacy Became a Human Right. - Human Rights Law Review 2014, 14 (3), p 442.
[179] T. Payton, T. Claypoole. Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. USA: Rowman and Littlefield 2014, p. 214.
[180] *Ibid*, p. 212.
[181]European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7.2.2013.

deeply integrated mobile computing growth worldwide[182]. Thus, the change of privacy attitudes that we have come to expect on computers (phones, at homes, or even bodies) is not due to huge government programs designed to spy. Instead, this change has occurred with new, comfortable and convenient technology that enables the advantages of infinite knowledge at person´s fingertips and constant connection to Internet.[183] This reason can be solved by relative legislation that may bring along change in individuals behaviour.

Moreover, the justifications by states presented another reason for distancing from the universal treaty requirements, it is that the UDHR is not legally binding and that the signatories of the treaty who had an «unprecedented number of reservations, understanding, and declarations» rendered the treaty powerless under domestic law.

Much of this discussion tilted to the question of power over advantages related to electronic data possession and processing. The electronic data became valuable asset, facilitator of economic growth[184] and enhancer of diplomatic negotiations. From the economic point, surveillance practices provide insight into other countries economic policy or behaviour which could affect global markets.[185] From a military perspective, the possession of surveillance assets provides the confidence to adequately assess the capabilities of a potential partner over time.[186] And finally, spying on the UN, European Union (hereinafter EU), the European Parliament, the G20 summit, the Vatican, and world leaders is aimed at gaining advantage in diplomatic negotiations.[187] These reasons ground the view that there are no better alternatives in the current digitized world for progressive states (United States (hereinafter US), United Kingdom (hereinafter UK), Canada) to effectively protect country's sovereignty than by advancing defence capacities of information technology and corresponding national legislation. These reasons do not serve that much to justify allowing interception to every individual and to set up a standard of overall intrusion of the right to

[182] T. Payton, T. Claypoole. Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family, p. 213.
[183] *Ibid*, p 227.
[184] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission. European Commission. Brussels, p. 2. 7.2.2013.
[185] A. Zaure. The Balance between Privacy, Freedom of Information, and National Security. -Jusletter IT. 28. 02. 2016, p 2. - http://jusletter-it.weblaw.ch/en/issues/2016/IRIS.html.
[186] D. Kearn. Great Power Security Cooperation: Arms Control and the Challenge of Technological Change. Lanham: Lexington Books 2015, p. 27–28.
[187] These Programs Were Never About Terrorism: They're About Economic Spying, Social Control, and Diplomatic Manipulation. They're About Power. -http://www.washingtonsblog.com/2013/12/programs-never-terrorism-theyre economicspying-social-control-diplomatic-manipulation-theyre-power.html, 17.12.2013.

privacy and freedom of information. Merely, covert activity of secret intelligence services has been present without any depending on terrorism or crime prevention justifications.

III Midway conclusions

Moreover, the electronic data aggregation facilitates counter-terrorism strategies which have a purpose to engage "control"-risk management in response to the treat of terrorism.[188] For this reason data aggregation and processing is usually managed by the intelligence agencies governed by governments, where supervision of interception by judges and prosecutors is limited and not open to public scrutiny. Much the same, the absence of requirement to notify the subject when surveillance had ceased further undermined the effectiveness of any available remedies against violations by the intelligence services. Also, private internet service providers usually manage under cooperation with state officials secretly to hand over a complex and often relatively complete «digital dossier»[189] of individuals as was evidenced in the Apple case when it was occasionally caught sharing a year's worth of location data on every user's iPhone with state officials.[190] These sorts of revelations are rarely met as they need to unified forces by individuals or organisations to be able to prove facts in order to protect rights in court procedure. Based on above, in order to shift the position of scales back to position which has been set for the international human rights treaties, an equally powerful response to the intrusive activities should be in place. Conclusively, there is a variety of reasons under which States prefer not to comply with the legal standards agreed after the Second World War.

[188] P. Fernandez-Sanchez. International Legal Dimension of Terrorism. Leiden, Boston: Martinus Publishers 2009, p 150.
[189] L. Gelman. Privacy, Free Speech, and «Blurryedged» Social Networks. - Boston College Law Review. Vol. 50. Issue 5. 2009, p. 1316.
[190] Devices that betray you. The TechPro Series 2014, p 27.

C Future International Standard Set

I Democracy at stake

The purpose of this chapter is to provide relevant recommendations on the potential balance. If these reasons that produced the opposing balances can be solved by means of international law, the thesis proposes recommendations on potential solutions to achieve unity and clarity of balances for the rights and national security to be considered as relevant standards for future practice.

Setting the proposals for a level at which it is comfortable for States to implement the laws, and human rights will not be jeopardised, is part of a current wider task of society. Rules established for what businesses and police can see and what processes are required for them to move beyond their basic level of access, serves future avoidance of the infringement of privacy.[191] Yet, while Payton and Claupoole hold an opinion that there is no expectation for businesses to hold back from taking full advantage of all the resources available to companies for profit and competitive advantage, they guess that Sun Microsystems CEO Sott McNealy saying "You have zero privacy anyway. Get over it" is self-serving for technology executive who would like to remove all barriers to gathering data.[192] Thus, the statement cannot be accepted as an impartial solution that meets interests and needs for the internet society as a whole or contributes to the sustainable legal order. At the same time in the US where business limits are clear, companies tend to stay within the lines of a business-centered approach.

Yet, laws have limits, and therefore cannot alone solve all the problems of privacy, freedom of information and national security. A constitutional guarantee alone cannot ensure meaningful exercise of rights in practice. If we do not have a practice that is supported by legal culture that is supportive of civil liberties, we cannot have civil liberties.[193] For that reason, some companies embody the insight that users should be in meaningful control of how their personal information is used and that transparency by commercial actors promotes

[191]T. Payton, T. Claypoole. Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family, p 229.
[192]*Ibid*, p 228.
[193]N. Richards. Intellectual Property: Rethinking civil liberties in the Digital Age. Oxford University Press 2015, p 169.

accountability and deters wrongdoing.[194] A leader in these efforts is the non-profit Mozilla Corporation and its mission, alongside the Firefox browser, is to respect the privacy[195] enshrined in European legal instruments.

At the same time, there are views that support the complex solutions approach that is complemented by multitasked components. Jack Balkin believes that decisions for regulated future[196] will not occur from constitutional laws, rather, they will be decisions about technological design, legislative and administrative regulations, the formation of new business models, and the collective activities of end-users.[197]

II Recommendations for Solutions

Whilst certainty is desirable, it may bring in its train excessive rigidity, and the law must be able to keep pace with changing circumstances. Thus, the thesis supports that general provisions of law can at times make for a better adaptation to changing circumstances than can attempts at detailed regulation.[198] Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague, and whose interpretation and application are questions of practice.[199] But the dangers inherent in prior restraints call for the most careful scrutiny.[200]

From the same viewpoint the recent EU developments in the field of counter-terrorism laws have revealed that the implementation of laws with regards to national security purposes tend to hold in favour of restricted interpretation. Thus, the European Commission's proposal, issued on 2 December 2015, argued that the EU Directive on combating terrorism does not meet adequate level of fundamental rights standards as it extends the scope of criminal law too far, for example, penalizing the receiving of training for terrorism by attending a training camp run by a terrorist association or group through various electronic media, including

[194] *Ibid*, p 182.
[195] *Ibid*, p 182.
[196] J. Balkin. The Future of Free Expression in a Digital Age. -Pepperdine Law Review. No 101. 2008. Cited in: M. Price, S. Verhulst, L. Morgan. Routledge Handbook of Media Law. Routledge. 2013, p 435.
[197] N. Richards. Intellectual Property: Rethinking civil liberties in the Digital Age, p 183.
[198] *Times Newspapers Ltd v. the United Kingdom*, nos.3002/03 and 23676/03, §§ 20, 21 and 38, ECHR 2009, where the "Internet publication rule" relied on a rule originally dating from the year 1849, and *Editorial Board of* Pravoye Delo *and Shtekel v. Ukraine*, no. 33014/05, §§ 60-68, ECHR 2011 (extracts), where the lack of reference to Internet publications in the otherwise quite detailed media law gave rise to an issue of lawfulness under Article 10 of the Convention.
[199] *Lindon, Otchakovsky-Laurens and July v. France* [GC], nos. 21279/02 and 36448/02, § 41, ECHR 2007-IV.
[200] Observer and Guardian v. the United Kingdom, judgment of 26 November 1991, Series A no. 216, p. 30, § 60.

through the Internet.[201] This positions led to the need of the more balanced view with objective and impartial solutions on future interpretations.

Therefore, the thesis sees that regulation for Internet matters should be construed as strict concepts partly due to political reasoning. Rather, compliance to the "quality of law" standard can be achieved by working out precise dominating concepts of primary institutions, responsibility sharing and guarantees related to such concepts as critical infrastructure and super-critical infrasture, armed conflict etc. Declaring these concepts in international political meetings is not mandatory, but elaborating and regulating them helps to draw clear lines within a country. Delineated understanding and clearness helps to define the range of state responsibility and promote legal certainty as the ECHR reiterates in this context that it is not its task to take the place of the domestic courts. The ECHR is satisfied that provisions along with the pertinent case-law should make clear the consequences of different chosen behaviours.

The thesis recommends that depending on the national legal traditions and structures dedicated to national security arrangements, the scope of the national security exemption must be clarified. The Working Party (hereinafter WP 29) suggested in three WP 29 opinions[202] that the clear definition of the concept of national security should be adopted by the European legislature, as it is not conclusive in the case law of the European courts. Therefore, a wide diversity of oversight models should be harmonised, to reduce disparity of the national legal traditions and structures dedicated to national security arrangements. While considering all remedies, the internal national security threats and external (foreign) national security threats should be addressed, to specify different responsibilities, civilian (Ministry of Interior or Justice) and military (Ministry of Defence). Thus, restrictions to the fundamental rights of all citizens need to be exercised according to a strict necessity and proportionality test which is a prerogative of a democratic society.

Additionally, the thesis urges to respect the data protection principles on the protection of personal data, usually included in the national constitutions of the Member States, by the intelligence services and thus by States, who are themselves bound with treaty obligations. Following the Snowden revelations, the thesis draws to attention that the borders of legality

[201]Proposal for a Directive of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism. 2015/0281 (COD). Available: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative documents/docs/20151202_directive_on_combatting_terrorism_en.pdf.
[202]No 14/EN WP 228, 14/EN WP 220 and 819/14/EN WP 215.

have been reached and even crossed since surveillance programmes are likely to exist in all parts of the world that may not be traceable and public authorities may have no sight of a coherent and consistent application of the data protection principles following the European Convention on Human Rights and Council of Europe Convention 108. On the other hand, this view should be considered carefully as it may not have a significant effect because public authorities might be more concerned with the secret intelligence services than with violating the rights of citizens and breaching state level obligations. While constantising a fact, governments should have serious intention to carry out actions to protect its citizens but rather to follow their political interests. In the divide between citizens and governments, citizens are troubling governments in fulfilling their legal obligations.

As a result, the thesis proposes to consider that implementation of the existing international standards with the additional protocol of Article 17 of the ICCPR. This suggestion is also supported by the EU Working Party WP29, that supposes that existing international agreements would grant adequate data protection safeguards to individuals when intelligence activities are carried out because: a) the interpretation of existing international treaties with the additional protocol of Article 17 of the ICCPR are able to support the global instruments providing for enforceable, high level privacy and data protection principles at time before the new global instrument will be accorded, and b) the convincing development of a global instrument providing for enforceable, high level privacy and data protection principles is necessary in order to fully address specific criteria settled for restrictions in a way that there are any violations related to surveillance of electronic communications for intelligence and national security purposes. As long as there is no relevant specified treaty, it cannot be said in a convincing manner that there are inter-State violations related to surveillance of electronic communications for intelligence and national security purposes.

III Proposed balance project for the future

A further suggestion on the potential additional protocol of Article 17 of the ICCPR will be introduced:

"*Being fully aware* of the already widespread and constantly increasing use of electronic data processing systems for records of personal data on individuals;

Recognising that, in order to prevent abuses in the storing, processing and dissemination of personal information by means of electronic data banks in the private sector, legislative measures may have to be taken in order to protect individuals;

Considering that it is urgent, pending the possible elaboration of an international agreement, at once to take steps to prevent further divergencies between the laws of member States in this field;

Having regard to Resolution on the protection of privacy in view of the increasing compilation of personal data into computers, adopted by the seventh Conference of European Ministers of Justice,

Recommends the governments of member States:

(a) to take all steps which they consider necessary to give effect to the principles set out in the Annex to this resolution;
(b) to inform the Secretary General of the Council of Europe, in due course, of any action taken in this field.

The following principles apply to personal information stored in electronic data banks in the public and private sector. For the purposes of this resolution, the term "personal information" means information relating to individuals (physical persons), and the term "electronic data bank" means any electronic data processing system which is used to handle personal information and to disseminate such information.

1. The information stored should be accurate and should be kept up to date. In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.

2. The information should be appropriate and relevant with regard to the purpose for which it has been stored.

3. The information should not be obtained by fraudulent or unfair means.

4. Rules should be laid down to specify the periods beyond which certain categories of information should no longer be kept or used.

5. Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.

6. As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

7. Every care should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way.

8. Precautions should be taken against any abuse or misuse of information. Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirections of information, whether intentional or not.

9. Access to the information stored should be confined to persons who have a valid reason to know it. The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy.

10. Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person."

Further recommendations on the system for judicial warrants are indicated. In other countries judicial interventions take place at the point of granting the warrant: it is common practice for warrants to be granted by judges rather than by politicians. We might consider adopting judicial authorization rather than judicial supervision to grant a greater safeguard for the individual. For example no-one would think that a minister should issue interception warrants. Also it is not clear why the current practice of an after event audit is better than a system of proper interrogation by a judge before a warrant is issued.[203] This way the tribunal is protected by any judicial review of its decisions, including decisions as to jurisdiction.

[203]A. Bradley, K. Ewing, C.Knight. Constitutional and Administrative Law. 16.Ed. Pearson 2015, p. 429.

The grounds for lawful authority are suggested as:

- The first option for lawful authority is where both sender and recipient consent to the interception. An example is in *R v Rasool*,[204] with the recording of a kidnapper telephoning in order to identify or trace the kidnapper. The operation is authorized as surveillance rather than by means of an interception warrant under relevant law.
- The second option of lawful interception takes place without any consent of either sender or the recipient by an undercover agent whose activities have been authorized under the specific legal ground which gives statutory authority for interception without a warrant to certain communications intercepted for specific reasons widely agreed in order to maintain public and private well-being, including under prison rules[205], in high-security psychiatric hospitals; and in specific crime investigation.
- The third basis for interception is with the authority of a warrant issued by the highest impartial authority whose responsibility is to provide a legally grounded warrant. There are three grounds for the issuing of a warrant: the interests of national security, the prevention or detection of a serious crime, and to give effect to an international mutual assistance agreement. According to the government, the request ”would have to satisfy the law of the requesting country as well as national interception law”. But that may not amount to much in practice if the law of the requesting country has few protections for foreign nationals (as where it is information about a national citizen that is required). The conduct authorized by the warrant must be proportionate to the end to be achieved, and before a warrant is granted consideration should take place to find if there is any other means to obtain information.

Flexibility of legal provisions, especially in international legal treaties, is welcome as then law can meet the larger scope of life incidents, as well it provides for law breathing space while it evolves with changing times and occasions.

The suggested propositions support establishing the “quality of law” standard as they encourage working out precise dominating concepts of primary institutions, responsibility sharing and guarantees related to such concepts as critical infrastructure and super-critical infrastructure, armed conflict. Thus, these recommendations delineate precise understanding and clearness that further help to define the range of state responsibility and promote legal certainty.

[204] *R v Rasool*, 1 WLR 1092 523, 1997.
[205] *R v Owen* (1999) 1 WLR 949.

It is seen that by accepting the proposed recommendations States will probably be more willing to meet the internationally binding standards if they have clear lines and accompanying enforcement mechanisms to sufficiently meet the internal and external national security threats. It is inevitable that the application of restrictions be exercised according to a strict necessity and proportionality test which is fundamental prerequisite of a democratic society.

By emphasizing the precondition of respect for the national constitutions on the data protection principles by intelligence services and thus by States to meet the obligation to act in good faith and not defeat the purpose of the ICCPR according to the customary international law.

As a result, the support of the implementation of the existing international standards with the additional protocol of Article 17 of the ICCPR might discipline States to provide adequate data protection safeguards for individuals meanwhile intelligence activities carry out their duties. Support favoring the global instruments will introduce the standard for privacy, freedom of information, and data protection principles which should not offer less protection online than they have protection offline. Accordingly, a treaty with specified provisions would ease implementation of globally agreed international standards, so diminish the threat of inter-state violations related to surveillance of electronic communications for intelligence and decrease possibility to attach State responsibility for operations necessary in national security protection.

While society might have a justifiable expectation for the protection and implementation of human rights at least to a minimum extent, it is essential to guarantee that the balance set by international human rights treaties will not be jeopardized, rather supported for the benefits of economical and social development, and equally for those who have an expectation for a free Internet society, and equally for those who believe that proliferation of data exchange on the Internet should be subject to justified limitations. Both views deserve equal respect and therefore it might be fully admitted that solutions for the future regulation[206] will be decisions about technological design, legislative and administrative regulations, the formation of new business models, and the collective activities of end-users.

[206] Jack Balkin. The Future of Free Expression in a Digital Age. -Pepperdine Law Review. No 101. 2008. Cited in: M. Price, S. Verhulst, L. Morgan. Routledge Handbook of Media Law. Routledge. 2013, p. 435.

While surveillance is used in security purposes, it is found that surveillance is not an absolutely effective tool in crime investigation as it was found that cameras cannot catch *important facts important* for investigation. For example robbers find places where cameras are turned other direction or commit to crime behind the corners or find another ways. Also in practice not so many people had chance to get security from crimes because of for example CCTV cameras. This way we find that massive surveillance is not justified as absolutely effective, but only as a supportive remedy in crime handling. The same logic could be followed with national security interests and terrorists investigation means where individuals are uncertain about how given powers will be used."

Conclusions

After terror attacks several States faced the paradigm shift for the balance of privacy and national security, similarly that in the US after 9/11 in 2001. Yet, the doctrine of "securitization" presents serious opposition to the existing balance established by the courts in the EU which fuels opposite views in the European and American balances between human rights and national security interests. The thesis indicated that there is an absence of a shared vision on the future of legitimate limitations of human rights in favor of national security interests that has resulted in a polar dichotomy between judicial, legislative and executive powers within European States. This trend inevitably endangers the existing understanding of democracy and the rule of law.

Apparently, the balance of rights has a dynamic character and is mainly affected by the volatile contextual framework of interests. All three notions involved in the discussion, the right to privacy, freedom of information, and national security, entail non-definable denominators which change context, but have a core essence which can be implemented in a technical environment such as the Internet. But, the core essence of international human rights is applicable to online environment as well. Thus, there is a variety of elements that affects the position of the values on scales.

The thesis introduces the fresh view of seeing the problem as a complex concept of the interrelationship of all three aspects applicable in cyber-matters as a three-dimensional paradigm that reflects emerging legal matters of electronic data processing and represents reality in the most adequate way. So far, the related matters have been seen mainly through a

two-sided approach, which may not be sufficient and may leave essential elements of the reality misaddressed.

The main question during the research was how to find a balance between the parallel demands of privacy, freedom of security, and national security in existing international legal instruments so that States would more likely follow them. Currently in the absence of a specific international treaty or convention, there are still common denominators for the right to privacy in online. If the right covers any activity concerning an individual´s data transmission via Internet the protection is included in the protection of the private sphere. For the protection of the freedom of information, the protection covers all kinds and sorts of expression and the means of their dissemination, even those that offend, shock, or disturb are also protected on the Internet. National security is perceived mostly as security from foreign powers, not from internal threats, and especially not from home-grown internal threats. Thus, it is possible to apply an approach to human rights online that is similar to that applicable offline.

For the achieved results on the balance set for the European region, ECtHR case-law emphasizes persistently: priority is given to national security interests only in those cases where interference with human rights was justified by passing a «triple» control test of necessity, legitimacy and proportionality by means of lawful limitations. Moreover, it has been indicated that this «European standard» of balance has exerted an influence on the majority of the world's countries, although it originated from the universal legal standards established in the UDHR and thus serves as a universal lawful standard enshrined in the universal human rights treaties. With regards to the balance between privacy and freedom of information, it can be concluded that the tendency of the ECtHR is to put individuals back in control by updating their data protection rights can be followed and that there is no ground for spreading the idea that the ECtHR allows for massive censorship.

While the thesis examined the balance of rights focused at an international level, several national regulations revealed divergent regional implementations of international standards and interpreted them in an incoherent manner. Through systematic analysis of the current practices of the most influential States and regions, such as those of the permanent members of the UN Security Council, the US, the UK, Russia, China, and France, we have shown that contradictions were still present.

In the US a noteworthy change in State practice was present. The 9/11 terrorist attacks caused a crucial shift in the balance for privacy, freedom of information, and national security in the US as these incidents created the greatest distinction between the EU and US approach caught through idea of the “exception”. Before the terrorist attacks to the US, their courts complied with the international human rights standards, but the 9/11 terrorist attacks imposed such a level of threat and gravity that it created the greatest distinction between the EU and US approach expressed through idea of the “exception”. As a result, during the Bush administration initiated “war on terror”, the US courts case-law started to decide in favour of national security interests causing the shift in the balance which was is seen as evasion and erosion of the rule of law.

Therefore it might be concluded that States have grouped into territorial collective unities with homogeneous solutions to handle new threats. While the UK adopted tough legislation intended to benefit State effectiveness in protecting its national security, a similar paradigm shift in the conceptualization of privacy and national security after 9/11 in 2001 in the US seems to have resulted in the UK following 7/7 in 2005. Before the terror incidents the case-law of the UK courts was designed to ensure that practices in surveillance were brought into line with the ECHR requirement that the different kinds of surveillance be authorized in advance and with judicial approval. The new Counter-Terrorism and Security Act 2015 allowed the interception of connection and intensely challenged in the UK without any prior judicial warrant. Under these provisions, the balance of privacy, freedom of information, and national security that is now present in US has already taken place in UK case-law. Therefore, the upcoming decisions of the ECtHR are to show the results of the cross-continental battle between legislative and executive powers with judicial ones.

The French adopted a new counter-terrorism law which legalized electronic surveillance by public bodies and increased the sentence to seven years if an offense is committed online. In January 2015 France doubled down on an existing law that allows the shutdown of websites deemed to be «sympathizing with terror». Thus, France has also implemented an interpretation of existing international instruments in favor of national security interests.

Similarly, Russia has contributed to the list of States that have decided to choose national security interests over the protection of human rights in cyberspace. Despite the proper limits of communications surveillance powers under Russian law, Russia’s State practice with the SORM system, which is present in Russia and other post-Soviet countries, is not consistent

with the requirements of Article 8 of the ECHR. Thus, Russia is one country that sits between the contradictory approaches of Europe and those, like Brazil, that are willing to save their political autonomy and protect human rights in the digital sphere according to the 'offline' human rights treaties.

As a result of China's specific attitude towards international law obligations, the implementation of data protection standards in China proceeds with distinctly Chinese characteristics where the perspective on national legislation on data protection is strongly tilted towards national security interests. Currently, data protection and privacy regulations in the online context might be considered as the most extensive and restrictive in the world.

The thesis revealed the reasons that States used to justify practicing online security measures contrary to the international treaties. These reasons could be solved by international law measures.

Among other provisions, the record search provision in the US made it possible for the FBI to secure client records without judicial oversight, and without prior notification of the person under surveillance. The accountability and oversight were not prioritized.[207] Thus, the US judicial concept of balance moved close to the legislative one - the completely opposite side from the previous position - and started to contradict the judicial balance established by the case-law in the ECtHR.

For the purpose of reducing the existing wide diversity of oversight models, the thesis recommends clarifying the scope of the national security exemption. So, the clear definition of the concept of national security should be adopted and the wide diversity of oversight models should be harmonized, to reduce disparity of the national legal traditions and structures dedicated to national security arrangements. The thesis proposes that restrictions to the fundamental rights of all citizens need to be exercised according to a strict necessity and proportionality test which is a prerogative of a democratic society.

As the dangers inherent in prior restraints call for the most careful scrutiny, the thesis supports the notion that general provisions of law can at times make for a better adaptation to changing circumstances than can detailed regulation. From the same viewpoint the recent EU

[207]D. McLeod, D. Shah. News Frames and National Security: Covering Big Brother. New York: Cambridge University Press 2015, p 1, 2.

developments in the field of counter-terrorism laws have revealed that the implementation of laws with regards to national security purposes tend to hold in favour of restricted interpretation.

The thesis proposes recommendations on potential solutions to achieve unity and clarity of balances for the rights and national security to be considered as relevant standards for future practice.

The thesis sees that the regulation of Internet matters should be construed as strict concepts partly affected by political reasoning. Rather, compliance to the “quality of law” standard can be achieved by working out precise dominating concepts of the primary institutions, responsibility sharing, and guarantees related to such concepts as critical infrastructure and super-critical infrastructure, armed conflict etc. While emphasizing a fact, governments should have the serious intention to carry out actions to protect its citizens but instead they follow their political interests. In the divide between citizens and governments, citizens are pushing governments to fulfill their legal obligations.

As a result, the thesis proposes the coherent implementation of the existing international standards by the means of the additional protocol of Article 17 of the ICCPR as it is essential to strike the balance between the parallel demands of privacy, freedom of security, and national security in international legal instruments so that they will be more willingly accepted by the leading States.

Thus, in order to resolve the present dichotomy of concepts for the balance between executive and judicial powers in Europe that cracks the existing framework of the European democracy, the thesis introduced the balance concept for the future with the addition of protocol of Article 17 of the ICCPR and the principles applicable to personal information stored in electronic data banks in the public and private sector.

Kokkuvõte

Mitmed terrorirünnakud USA-s 2001 aastal tõid endaga kaasa paradigma muutuse privaatsuse, infovabaduse ja riigi julgeoleku tasakaalus. Sarnased muutused kaasnesid ka teistes riikide, kaasa arvatud Ühendkuningriik ja Prantsusmaa. Samas, laiaulatuslik terroriohu ning kuritegevuse ennetus ning sellega võitlus „julgeoleku" kaalutlustel põhjustavad tõsist lahkheli olemasoleva inimõiguste ja riikliku julgeoleku tasakaalu suhtes, mis on loodud rahvusvaheliste inimõiguste instrumentide tõlgenduste tulemusena, põhjustades tugevat lahkheli Euroopa Inimõiguste Kohtu, Euroopa Liidu Kohtu ning USA, Venemaa, Suurbritannia ja Hiina kõrgema astme kohtute tõlgenduste vahel. Magistritöö peegeldab õiguslikku kontrasti automatiseeritud andmetöötluse praktika kohaldamise suhtes, kus rahvusvaheliselt tunnustatud inimõiguste suhtes kohaldatakse täiesti erinevat kontseptsiooni. Nimelt, Euroopa andmekaitse põhimõtteks on rahvusvaheliste inimõiguste, ennekõike privaatsuse ja infovabaduse eelistus riikliku julgeoleku huvide suhtes, mida kohaldatakse ning peetakse õigustatuks kolmeastmelise kontroll-testi läbimise järel: proportsionaalsus, vajalikkus ning õiguspärasus. Teiste sõnadega, vaid siis on põhjendatud inimõiguse riive, kui see on läbinud nimetatud õiguspärase sekkumise kontrollfiltri. Pärast USA terrorirünnakuid, nimetatud tasakaal privaatsuse ja riikliku julgeoleku vahel pöördus vastupidiseks sellele, mis juhindus ÜRO Kodanike- ja Poliitiliste Õiguste Paktist, millega on Euroopa seadusandlus ja täidesaatev võim kooskõlas. Sarnaselt, USA trendiga liitusid ja Ühendkuningriik ja Prantsusmaa. Hiina ja Venemaa on siinkohal autori arvates erandlikud, kuna on riikliku julgeoleku huve õigusliku konflikti oludes eelistanud inimõiguste kaitsele ajaloolistel kaalutlustel. Nimetatud tendents on progresseeruv ning haarab endaga infotehnoloogia võimekuselt arenevad riigid, mis omakorda paratamatult ohustab olemasolevat arusaamist demokraatiast ja õigusriigi põhimõtet.

On tõenäoline, et fragmentaarne jaotumine rahvusvaheliste nõuete täitmise osas jääb alles, kuid fundamentaalsetes küsimustes äärmuslikku polaarsust põhjustavates vaadetes tuleb leida kompromiss. Magistritöö eesmärgi täitmiseks esitleti kompromissi ÜRO Kodanike- ja Poliitiliste Õiguste Pakti artikkel 17 protokolli vormis, kaasnevate definitsioonidega “isikuandmed“ ja “andmepank“ jaoks. Arvestades Interneti riigiülest iseloomu ning riikide ühise koostöö potentsiaali, on lahenduseks ainumõeldav riikidevaheline kokkulepe, mis arvestab esilekerkinud vastakate vastuseisude põhjusi, lähtub riikide vajadustest ning pakub maksimaalsel viisil tasakaalustatud kompromisse. Just selleks esitleti käesoleva magistritöö uurimisega nimetatud protokolli projekt. Täiendavalt, õigusliku lahenduse õigustuseks räägib

ka põhjus, et riikideüleselt kokkulepitud õigusliku instrumendi mõju avaldab nii õigusandliku, kohtu- kui täidesaatva võimu poolt harmoonilisele inimõiguste kaitsele, nii riigisiseselt, regionaalsel kui kontinentaalsel tasemel.

Magistritöö leidis, et Euroopa inimõiguste kohus ja Euroopa Liidus on tasakaalu privaatsuse kaitses, infovabaduse ja riikliku julgeoleku kolmnurksuhtes kohaldanud järjekindlusega ka Interneti keskkonda puudutavate õiguste ja huvide põrkumiste korral. See tähendab, et õiguste kaitse tagatised on Euroopa kohtute tasandil jäänud muutumatuks. Erinev on olukord USA jaoks, mis pärast 2001 terrorirünnakuid USA-s, muutis regionaalset seadusandlust, mis muutsid inimõiguste ja nende erandite omavahelist suhet. Selle tulemusena riiklik julgeolek digitaalse kommunikatsiooni juhtudel ületab inimõiguste kaalutlusi. Sarnaselt, magistritöös uuritud Ühendkuningriik ning Prantsusmaa järgivad praktikat, mis toetub vastavale siseriiklikule seadusandlusele. Õiguskirjanduses on välja toodud, et ka teised Euroopa Ühenduse riigid peavad vajalikuks isikuandmete töötlemist rikkudes Euroopa Ühenduse andmetöötluse õigusreegleid, riikliku julgeoleku kaalutlustel, kujundades selliselt rahvusvahelist praktikat. Seega, võib jõuda seisukohale, et täidesaatva, kohtu- ja seadusandlike võimude lahkheli inimõiguste ja riikliku julgeoleku suhte küsimustes on laiem kui riiklikul või regionaalsel tasemel, Euroopa Liidu kohtu lahendid on vastuolus ka siseriiklike kohtulahenditega, nagu oli märgata Ühendkuningriigi ja Prantsusmaa juhtudel. Magistritöö autor on seisukohal, et riikide praktika tendents on demokraatliku senikehtinud tasakaalu ohustav ning võib tuua kaasa kontrollmehhanismide kohaldamist, mis ei ole kooskõlas kaasaja ühiskonna õigusriiklike tõekspidamistega.

Magistritöö autor annab au arusaamisele, et riikliku julgeoleku strateegiliste kontseptsioonide polaarsus ei saa olla lahendatud vaid rahvusvahelise mõjuga õigusliku instrumendi tõlgendusega nõustumisega ÜRO-s. Kuid püstitatud uurimisküsimuse lahendamiseks, kuidas leida tasakaal paralleelsete huvide nagu privaatsus, infovabadus ja riiklik julgeolek, lahendamiseks autor pakub ÜRO Kodanike- ja Poliitiliste Õiguste Pakti artikkel 17 ühetaolise tõlgenduse kokkuleppe projekti, ning pakub definitsioonide “isikuandmed“ ja “andmepank“ sõnastust.

2012. a ÜRO inimõiguste Resolutsioon deklareeris, et kõik inimõigused kehtivad ka online keskkonnas. Küsimusele, kuidas inimõigusi saab tõlgendada digitaalse keskkonna kontekstis, autor vastas esmalt, millised on privaatsuse, infovabaduse ja riikliku julgeoleku huvide olemuse elemendid, mida saab kohaldada Internetiga seoses. Järgnevalt uuriti, millised on

omavahelised suhtes õigustel omavahel ning omakorda riikliku julgeoleku huvidega. Autor vaatas kõiki küsimusi läbi kolmetahulise prisma, kus privaatsus, infovabadus ja riikliku julgeoleku huvid on omavahel põimunud ning moodustavad identifitseeritava ruumi kohtupraktika tõlgendustele tuginevalt. Peamiselt uuriti Euroopa Inimõiguste praktikat, Euroopa Liidu Kohtu praktikat, mille pinnalt järeldati prisma piirid. Sellist käsitlust toetab veendumus, mis pooldab ÜRO Kodanike- ja Poliitiliste Õiguste Pakti tasakaalu inimõiguste ja nende suhtes kohalduvate erandite suhtes, kuna see tasakaal on läbi erinevate ohtu loovate aegade ajaloos olnud vastupidav, on ka praegustes oludes põhjust olemasolevat korda säilitada ning sellest riikide poolt kinni pidada.

Magistritöö probleemipüstitus pärineb vaatest, mille kohaselt küberküsimustes isikuandmete levikuga internetis ja privaatsuskaitse ulatust puudutavate küsimuste lahendamisel piiriüleses kontekstis, nagu seda Internet on, ei saa enam piirduda kahe-tasandilise vaatega. Selle asemel Internetis sisalduvate isikuandmete piiriülese rahvusvahelise regulatsioon peaks peegeldama kõikide oluliste elementide kaalutud tulemust.

Õigus privaatsusele digitaalses inforuumis hõlmab igasugust isikuandmete töötlemist Interneti kaudu. Infovabaduse kaitse ulatub igasugusele mõtete, tunnete ning muude isiku väljendustele, sõltumata nende õiguspärasusest, ning viisidele, mille abil neid levitatakse. Kaasaja riikliku julgeoleku huvide kaitse on iga riigi osas väga erinev, kuid olemuse elementidena saab välja tuua riigi olemasolu ja säilimise tagamise kaalutlused laiaulatuslike ohtude suhtes, nii sise- kui välisohtude kontekstis.

Järgnevalt uuriti, mis on olnud põhjused valikuteks riikide poolt rahvusvaheliste õiguste instrumentide põhimõtetest eemaldumiseks inimõiguste ja nende suhtes kohalduvate erandite tasakaalu kontekstis. Töö käigus selgus, et ühelgi põhjusel ei saa olla mõju, mis oleks välistanud olemasolevate põhimõtete kohaldamist tasakaalu mõistes, ning need on lahendatavad kompleks lahenduste abil, poliitilised, diplomaatilised, õiguslikud ning vajalike infotehnoloogia meetmete vastuvõtmisega Interneti arhitektuuri muutmiseks.

Käesoleva magistritöö puudutab laiahaardelist probleemide ringi, kus tekib hulgaliselt ulatuslikke uurimisküsimusi, mis vajaksid põhjalikku uurimist, mida autor loodab teha järgmises õppeastmes.

Abbreviations

1. ECHR – European Convention on Human Rights
2. ECtHR – European Court of Human Rights
3. UDHR – Universal Declaration of Human Rights
4. OSCE- Organization for Security and Co-operation in Europe

Reference

1) Legal instruments

Binding:

1. African Charter on Human and People´s Rights European Court of Human Rights
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
3. Convention for the Protection of Human Rights and Fundamental Freedoms
4. Covenant on the Civil and Political Rights
5. Universal Declaration of Human Rights
6. European Convention on Human Rights
7. Resolution 59 (I). UN General Assembly. 14.12.1946

Recommendations:

8. United Nations General Asembly. The right to privacy in the digital age. A/RES/68/167. 21 January 2014
9. The UN Guidelines Concerning Computerized Personal Data Files. Doc E/CN.4/1990/72, 20.2.1990.-http://www.un.org/documents/ga/res/45/a45r095.htm, 14.12.1990
10. The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Paris 1980.-https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
11. Centre for Civil and Political Rights (CCPR) General Comment No. 16. (General Comments)
12. Article 19. The Johannesburg principles on national security, freedom of expression and access to information. November 1996
13. General Comment No 34 on freedom of opinion and expression 2011. UN Human Rights Committee. CCPR/C/GC/34, para 11. http://www.ohchr.org/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf.

14. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 17.04.2013. - http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/23/40 (16.02.2016)
15. Centre for Civil and Political Rights (CCPR) General Comment No. 16. (General Comments)
16. General Comment No 34 on freedom of opinion and expression 2011. UN Human Rights Committee. CCPR/C/GC/34, para 11. http://www.ohchr.org/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf
17. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/17/27. - http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/17/27 (16.02.2016)
18. Постоянное представительство Российской Федерации в ООН и других международных организациях в Женеве. нформация резолюции , принятой Генеральной Ассамблеей 18 декабря 2013 68/167 . Право на неприкосновенность частной жизни в цифровую эпоху. 9 апреля 2014 г., http://www.ohchr.org/Documents/Issues/Privacy/Russia.pdf

2) Monographies and scholars articles:

1. Akhavan, N. Electronic Iran: The Cultural Politics of an Online Evolution. Rutgers University Press. 2013.
2. Article 19. The Johannesburg principles on national security, freedom of expression and access to information. November 1996.
3. Balkin, J. The Future of Free Expression in a Digital Age. -Pepperdine Law Review. No 101. 2008. Cited in: M. Price, S. Verhulst, L. Morgan. Routledge Handbook of Media Law. Routledge. 2013.
4. Birkinshaw, P. Freedom of Information: The Law, the Practice, and the Ideal. Cambridge: Cambridge University Press. 4. Ed. 2010.
5. Cameron, I. National Security and the European Convention on Human Rights. Iustus Förlag: 2000.
6. Coliver, S. National Security and the Right to Information. 11 December 2012. - https://www.opensocietyfoundations.org/sites/default/files/coliver-nsp-pace20121220.pdf (18.12.2014).
7. Davis, D. David Davis: Parliament insulted our democracy with surveillance bill. 2407.15. -http://www.wired.co.uk/news/archive/2015-07/24/david-davis-dripa-judicial-review (22.03.2016).

8. Diggelmann, O. M. Cleis. How the Right to Privacy Became a Human Right. -Human Rights Law Review 2014. No 14.
9. Doswald-Beck, L. Human Rights in Times of Conflict and Terrorism. Oxford: Oxford University Press 2011.
10. European Court of Human Rights. New technologies. Factsheet. September 2014. - http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf. (18.12.2014).
11. Holmes. K. What is National Security? Index of US Military Strength 2015. - http://index.heritage.org/military/2015/important-essays-analysis/national-security/ (18.12.2014).
12. Kelly, S. and others. Privatizing Censorship, Eroding Privacy. Freedom on the Net 2015. - https://freedomhouse.org/report/freedom-net-2015/freedom-net-2015-privatizing-censorship-eroding-privacy (16.04.2016).
13. Kilkelly, U.The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights. Human rights handbooks, No. 1. Directorate General of Human Rights Council of Europe. 2003.
14. La Rue, F. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 17 April 2013. - http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/23/40 (16.02.2016).
15. Lester and D. Pannick (Ed). Human Rights Law and Practice. London: Butterworth 2004, para 4.82.
16. La Rue, F. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 17 April 2013. - http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/23/40 (16.02.2016).
17. Tikk-Ringas, E. Norms for International Peace and Security: Privacy, Freedom of Information and National Security. ICT4Peace Norms Project. April 2015. - https://www.gccs2015.com/sites/default/files/documents/Working%20PaperPrivacy,%20Freedom%20of%20Information%20and%20National%20Security.pdf (16.02.2016).
18. Tikk-Ringas, E. Comprehensive Normative Approach to Cyber Security. ICT4Peace Norms Project. April 2015. - https://www.gccs2015.com/sites/default/files/documents/ICT4Peace%20concept%20paper%20a%20comprehensive%20normative%20approach%20to%20cyber%20security.pdf (16.02.2016).

19. Malanczuk, P. Freedom of Information and Communication. -Max Planck Encyclopedia of Public International Law. April 2011.
20. Moraes, C. Draft Report on the US NSA surveillance programme. European Parliament. No 2013/2188(INI). 8.01.2014.
21. Velu, C. The European Convention on Human Rights and the Right to Respect for Private Life, the Home and Communications. Cited in: R. White, C. Ovey. The European Convention on Human Right. 5th Ed., Oxford Univeristy Press.
22. Voorhoof, D. The Right to Freedom of Expression and Information under the European Human Rights System: Towards a more Transparent Democratic Society. RSCAS 2014/12 2014. Robert Schuman Centre for Advanced Studies Centre for Media Pluralism and Media Freedom, p 1. - http://cadmus.eui.eu/bitstream/handle/1814/29871/RSCAS_2014_12.pdf?sequence=1 (16.03.2016).
23. White, R. Ovey, C. The European Convention on Human Right. 5. Ed. Oxford Univeristy Press: 2010.
24. Wamala, F. ITU National Cybersecurity Strategy Guide. September 2011. - http://www.itu.int/ITUD/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (18.12.2014).
25. Ziolkowski, K. (Ed). Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. Tallinn: NATO CCD COE Publication 2013.
26. The Cyber Index International Security Trends and Realities. UNIDIR/2013/3. New York, Geneva: United Nations Institute for Disarmament Research 2013. - http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (18.12.2015).
27. Top 10 Internet-censored countries. -USA Today 5.02.2014.- http://www.usatoday.com/story/news/world/2014/02/05/top-ten-internecensors/5222385/.
28. Myth-busting: The Court of Justice of the EU and „the right to be forgotten. European Commission, p 4. -http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_rtbf_mythbusting_en.pdf (18.04.2015).
29. UN General Assembly. Report on the promotion and protection of the right to freedom of opinion and expression. A/68/362. 4 September 2013.

30. Toulson, R.. Freedom of expression and Privacy. Vol 41. Issue 2. London: 2007 (Paper presented at Association of Law Teachers Lord Upjohn Lecture. London. 9.02.2007).
31. General Comment No 34 on freedom of opinion and expression 2011. UN Human Rights Committee. CCPR/C/GC/34. http://www.ohchr.org/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf (14.02.3016).
32. General Comment No 11 on prohibition of propaganda for war and inciting national racial or religious hatred 1983, UN Human Rights Committee- http://www.ohchr.org/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf (15.03.2016).
33. Fernandez-Sanchez., P. International Legal Dimension of Terrorism. Leiden, Boston: Martinus Publishers 2009.
34. Kaye, D. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. A/HRC/29/32. 22.05.2015.
35. Freedom House. Vietnam: freedom of the press. - https://freedomhouse.org/report/freedom-press/2015/Vietnam, 2015.
36. Kelly, S. and others. Privatizing Censorship, Eroding Privacy. Freedom on the Net 2015. - https://freedomhouse.org/report/freedom-net-2015/freedom-net-2015-privatizing-censorship-eroding-privacy (16.04.2016).
37. Human Rights Watch Submission: World Development Report on Internet for Development. Human Rights Watch. - https://www.hrw.org/news/2015/08/26/human-rights-watch-submission-world-development-report-internet-development, 26.08.2015.
38. Freedom House.Vietnam: freedom of the press. 2015. Available: https://freedomhouse.org/report/freedom-press/2015/vietnam.
39. Kelly, S. M. Earp, L. Reed, A.Shahbaz, M. Truong. Freedom on the Net 2015. Privatizing Censorship, Eroding Privacy. -https://freedomhouse.org/report/freedom-net-2015/freedom-net-2015-privatizing-censorship-eroding-privacy.
40. Human Rights Watch. Human Rights Watch Submission: World Development Report on Internet for Development. -https://www.hrw.org/news/2015/08/26/human-rights-watch-submission-world-development-report-internet-development, 26.08.2015.
41. Bradbury, S. Balancing Privacy and Security. -http://www.harvard-jlpp.com/wp-content/uploads/2015/02/Bradbury_Final.pdf (30.03.2016).

42. Working Draft. Office of the Inspector General. ST-09-0002.- http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection (24.03.2016).
43. Electronic Privacy Information Center. Foreign Intelligence Surveillance Act (FISA). - https://epic.org/privacy/terrorism/fisa/.
44. Murphy, C. EU Counter-Terrorism Law: Pre-Emption and the Rule of Law. Oxford: Hart Publishing 2012.
45. McLeod, D., Shah, D. News Frames and National Security: Covering Big Brother. New York: Cambridge University Press 2015.
46. GCHQ does not breach human rights, judges rule. -BBC News 5.12.2014. - http://www.bbc.co.uk/news/uk-30345801.
47. Home Secretary Theresa May on counter-terrorism. Royal United Services Institute. - https://www.gov.uk/government/speeches/home-secretary-theresa-mayon-counter-terrorism, 24.11.2014.
48. Bradley, A.. Ewing, K. Constitutional and Administrative Law. 14. Ed. Harlow: Pearson Longman.
49. Fishman, A. Greenwald, G. Spies Hacked Computers Thanks to Sweeping Secret Warrants, Aggressively Stretching U.K. Law. -The Intercept_. - https://firstlook.org/theintercept/2015/06/22/gchq-reverse-engineering-warrants/, 22.06.2015.
50. Holehouse, M. Counter-terrorism Bill: What it contains. -The Telegraph 26.11.2014.- http://www.telegraph.co.uk/news/worldnews/islamic-state/11254950/Counter-terrorism-Bill-What-itcontains.html.
51. Clark, L. UK mass surveillance laws are unlawful, it's official. - http://www.wired.co.uk/news/archive/2015-07/17/uk-surveillance-laws-are-unlawful, 17.07.15.
52. Anderson, D. A Question of Trust. Report of the Investigatory Powers Review 2014.- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf (30.01.2016).
53. RUSI. A Democratic Licence to Operate Report of the Independent Surveillance Review. London, Brussels: Royal United Services Institute for Defence and Security Studies 2015.- https://www.rusi.org/downloads/assets/ISR-Report-press.pdf.
54. What price privacy now? The first six months progress in halting the unlawful trade in confidential personal information. -https://ico.org.uk/media/about-the-ico/documents/1042392/what-price-privacy-now.pdf, 13.12.2006.

55. Cameron, I. National Security and the European Convention on Human Rights. Uppsala: Iustus Förlag. 2000.
56. Masi, A. France's Online War on Terror Sympathizers and Extremists Has A New Cyber Security Cell. -International Business Times. -http://www.ibtimes.com/frances-online-war-terror-sympathizers-extremists-has-new-cyber-securitycell-1786662, 17.01.2015.
57. The Joint Supervisory Body of EUROPOL. Opinion 08/44 of the JSB in respect to the data protection level in the Russian Federation. - http://www.europoljsb.europa.eu/media/213359/0844%20jsb%20europol%20opinion%20on%20dp%20level%20in%20russian%20federation.en.pdf, 8.10.2008.
58. Private Interests: Monitoring Central Asia. Special Report. - https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf, 11.2014.
59. France faces 'litmus test' for freedom of expression as dozens arrested in wake of attacks. -https://www.amnesty.org/en/latest/news/2015/01/france-faces-litmus-test-freedom-expression-dozens-arrested-wake-attacks/, 16.01.2015.
60. UN Treaty Bodies and China. -Human Rights and China. - http://www.hrichina.org/en/un-treaty-bodies-and-china (13.04.2016).
61. Sceats, S., Breslin, S. China and the International Human Rights System. Chatham House. October 2012. - https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/r1012_sceatsbreslin.pdf (13.03.2016).
62. How Censorship Works in China: A Brief Overview. - https://www.hrw.org/reports/2006/china0806/3.htm (14.03.2016).
63. Zhou, Z. China's Draft Cybersecurity Law. The Jamestown Foundation. - http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44924&cHash=db05078399a49339345c2957196d4073#.VyUAwdR968o, 21.11.2015.
64. China. Country Report. Freedom on the Net 2015. - https://freedomhouse.org/report/freedom-net/2015/china.
65. O'Brien, D. China's name registration will only aid cybercriminals. Committee to Protect Journalists blog. - https://cpj.org/blog/2012/12/chinas-name-registration-will-aid-not-hinder-cyber.php, 28.12.2012.
66. Wong, Chun. China Adopts Sweeping National-Security Law. -The Wall Street Journal. -http://www.wsj.com/articles/china-adopts-sweeping-national-security-law-1435757589. 1.07.2015.

67. Lum, T., Figliola, P., Weed. M. China, Internet Freedom, and U.S. Policy. - Congressional Research Service. -https://www.fas.org/sgp/crs/row/R42601.pdf, 13.07.2012.
68. Human Rights Watch, China, “Race to the Bottom” Corporate Complicity in Chinese Internet Censorship”, August 2006, http://www.hrw.org/reports/2006/china0806/china0806webwcover.pdf.
69. China. Freedom of the Net. 2013. - https://freedomhouse.org/sites/default/files/resources/FOTN%202013_China.pdf (16.03.2016).
70. China: “Race to the Bottom”: Corporate Complicity in Chinese Internet Censorship. Human Rights Watch. - http://www.hrw.org/reports/2006/china0806/china0806webwcover.pdf, 08.2006.
71. Diggelmann, C., Cleis, M. How the Right to Privacy Became a Human Right. - Human Rights Law Review 2014, 14 (3).
72. Payton, T., Claypoole. T., Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. USA: Rowman and Littlefield 2014.
73. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission. European Commission. Brussels 7.2.2013.
74. Kearn, D. Great Power Security Cooperation: Arms Control and the Challenge of Technological Change. Lanham: Lexington Books 2015.
75. These Programs Were Never About Terrorism: They’re About Economic Spying, Social Control, and Diplomatic Manipulation. They’re About Power. - http://www.washingtonsblog.com/2013/12/programs-never-terrorism-theyre economicspying-social-control-diplomatic-manipulation-theyre-power.html, 17.12.2013.
76. Gelman, L. Privacy, Free Speech, and «Blurryedged» Social Networks. - Boston College Law Review. Vol. 50. Issue 5. 2009.
77. «Devices that betray you». The TechPro Series 2014.
78. Richards, N. Intellectual Property: Rethinking civil liberties in the Digital Age. Oxford University Press 2015.
79. McLeod, D., Shah, D. News Frames and National Security: Covering Big Brother. New York: Cambridge University Press 2015.
80. Zaure, A. The Balance between Privacy, Freedom of Information, and National Security. -Jusletter IT 2016.

81. Zhou, L. Chinese cyber regulators are getting personal.-Business Insider 4.02.2015. - http://www.businessinsider.com/chinese-cyber-regulators-are-getting-personal-2015-2?IR=T (18.04.2015)

3) Case-law

European Court of Human Rights:

1. *A. v. France*, 14838/89, 23 November 1993.
2. *Autronic AG v. Switzerland*, 22 May 1990, 12726/87.
3. *A. v. Norway*, 28070/06, para 64, 9 April 2009.
4. *Axel Springer AG v. Germany*, 39954/08.
5. *De Haes and Gijsels v. Belgium*, 24 February 1997, 19983/92.
6. *Halford v. the United Kingdom*, 20605/92.
7. *Raichinov v Bulgaria* 47579/99 20, April 2006.
8. *Observer and Guardian v. the United Kingdom*, 13585/88, 26 November 1991.
9. *Ahmet Yildirim v. Turkey*. 3111/10, 18 December 2012.
10. *Rehman v Secretary of State*, 2002.
11. *Herczegfalvy* v. *Austria* 10533/8324, September 1992.
12. *Steel and Others* v. *UK* 24838/94, 23 September 1998.
13. *Hashman and Harrup* v. *UK*, 25594/94, 25 November 1999.
14. *Gaweda* v. *Poland*, 26229/9514, March 2002
15. *Rekvényi v. Hungary*, 25390/94.
16. *Goussev and Marenk v. Finland*, 35083/97, 17 January 2006.
17. *Štefanec v. the Czech Republic* 75615/01, 18 July 2006.
18. *Delfi vs Estonia* case 64569/09, 18 July 2006.
19. *Groppera Radio AG and Others v. Switzerland*, judgment of 28 March 1990.
20. *Goodwin v. the United Kingdom*, 17488/90, 27 March 1996.
21. *Dzhavadov* v. *Russia*, 30160/04, 27 September 2007.
22. *Times Newspapers Ltd v. the United Kingdom*, 3002/03 and 23676/03.
23. *Lindon, Otchakovsky-Laurens and July v. France*, 21279/02 and 36448/02.
24. *Observer and Guardian v. the United Kingdom*, 26 November 1991.
25. *Hertel v. Switzerland*, 25 August 1998.
26. *Steel and Morris v. the United Kingdom*, 68416/01.
27. *Mouvement raëlien suisse v. Switzerland*, 16354/06.
28. *Animal Defenders International v. the United Kingdom*, 48876/08. 22 April 2013.

29. *Hachette Filipacchi Associés v. France*, 71111/01, 14 June 2007.
30. *MGN Limited v. the United Kingdom*, 39401/04. 18 January 2011.
31. *Axel Springer AG*, 39954/08, 7 February 2012.
32. *Von Hannover v. Germany* 40660/08 and 60641/08.
33. *Timciuc v. Romania* 28999/03,12 October 2010.
34. *Mosley v. the United Kingdom*, 48009/08, 10 May 2011.
35. *Google Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD),* C-131/12,13 May 2014.
36. *Pfeifer v. Austria*, 12556/03, 15 November 2007.
37. *Polanco Torres and Movilla Polanco v. Spain*, 34147/06, 21 September 2010.
38. *Peck v. United Kingdom*, 44647/98, 28 Jan 2003.
39. *Animal Defenders International v. the United Kingdom*, 48876/08, 22 April 2013.
40. *R.* v. *Spencer* 34644, 2014.
41. *Peck v. the United Kingdom* 44647/98, 28 January 2003.
42. *S. And Marper UK*, 30562/04 and 30566/04.
43. *The Sunday Times* v. *United Kingdom*, 538/74, 26 April 1979.
44. *Halford v United Kingdom*, 1997 24 EHRR 523.
45. *Roman Zakharov v. Russia*. Application no. 47143/06, 4 December 2015.
46. *R v Effic*, 1995 1 AC 309.
47. *Times Newspapers Ltd v. the United Kingdom*, nos.3002/03 and 23676/03.
48. *Editorial Board of* Pravoye Delo *and Shtekel v. Ukraine*, no. 33014/05.
49. *Lindon, Otchakovsky-Laurens and July v. France*, 21279/02 and 36448/02.
50. Observer and Guardian v. the United Kingdom, 26 November 1991.
51. 10 Human Rights Organisations and Others v. the United Kingdom, 24960/15.

US Supreme Court:

52. US Supreme Court, McIntyre v. Ohio Elections Commission, 1995.
53. United States Court of Appeals, *Yahoo! Inc v La Ligue Contre le Racisme et l'Antisemitisme*, C-00-21275JF, 2006.

UK Courts

54. Decision of England and Wales High Court (Administrative Court) nr. CO/4241/2008
55. *Mohamed, R v Secretary of State for Foreign & Commonwealth Affairs*, 21 August 2008.

56. *R. v. Department of Health, Ex Parte Source Informatics Ltd*., 2000, http://medlaw.oxfordjournals.org/content/8/1/115.full.pdf.
57. *Secretary of State for the Home Department v. Rehman*, 11 October 2002 http://www.1cor.com/1315/?form_1155.replyids=489.

Canada

58. Supreme Court of Canada, *R.* v. *Spencer*, SCC 43, 2014, 13.06.2014.

Korea

59. Korea Decision 2010 Hun-Ma 47, 252 (consolidated) announced 28 August 2012

Court of Justice of the European Union

60. ECJ *Digital Rights Ireland and Seitlinger and Others*, C-293/12 and C-594/12, 8 April 2014.

Keywords: Cyber security, civil liberties, privacy, national security, freedom of information, surveillance

Non-exclusive licence to reproduce thesis and make thesis public

I, Agnes Zaure,

1.herewith grant the University of Tartu a free permit (non-exclusive licence) to:

1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright, Application of International Human Rights online-Balance for Privacy, Freedom of Information, and National Security,

supervised by dr iur Eneken Tikk Ringas and co-supervised by professor Lauri Mälksoo,

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, Estonia
02.05.2016

_____