Vilnius University Faculty of Law

Department of Public Law

Mariami Tchikadze

2nd study year, International and European Law Study Program Student

Master's Thesis

National security as a ground to restrict human rights under the ECHR

Nacionalinis saugumas kaip pagrindas riboti žmogaus teises pagal EŽTK

Supervisor: Associate Professor Doctor Donatas Murauskas

Reviewer: Lina Urbaitė

Vilnius

2025

ABSTRACT AND KEYWORDS

The present Master's thesis analyzes national security as one of the legitimate grounds for restricting the right to privacy under Article 8 of the European Convention on Human Rights in the context of secret surveillance measures. It examines the scope of the margin of appreciation afforded to national authorities when implementing targeted and mass (bulk) surveillance regimes to protect their national security from internal and/or external threats. The thesis also identifies the key factors influencing the breadth of this margin as reflected in the case-law of the European Court of Human Rights.

Keywords: national security, right to privacy, targeted surveillance, mass surveillance, margin of appreciation.

SANTRAUKA IR RAKTINIAI ŽODŽIAI

Šiame magistro darbe analizuojamas nacionalinis saugumas kaip vienas iš teisėtų pagrindų apriboti teisę į privatumą pagal Europos žmogaus teisių konvencijos 8 straipsnį slapto sekimo priemonių kontekste. Jame nagrinėjama nacionalinių valdžios institucijų diskrecijos apimtis įgyvendinant tikslinius ir masinius (masinio) sekimo režimus, siekiant apsaugoti savo nacionalinį saugumą nuo vidinių ir (arba) išorinių grėsmių. Darbe taip pat nustatomi pagrindiniai veiksniai, darantys įtaką šios diskrecijos apimčiai, kaip atsispindi Europos Žmogaus Teisių Teismo praktikoje.

Raktiniai žodžiai: nacionalinis saugumas, teisė į privatumą, tikslinis sekimas, masinis sekimas, diskrecijos riba.

TABLE OF CONTENTS

INTRODUCTION

States frequently invoke national security to justify surveillance measures that interference with the right to privacy under Article 8 of the European Convention on Human Rights (hereinafter – the ECHR). In surveillance-related cases before the European Court of Human Rights (hereinafter – the ECtHR), the central question is how to strike a fair balance between an individual's right to privacy and the state's interest in protecting national security, particularly when it comes to external threats. The ECtHR does so primarily through the application of two interrelated legal doctrines: the margin of appreciation and the principle of proportionality, which require that the impugned measure must be a necessary and proportionate means to achieve the legitimate aims pursued.

It is important to note that the ECtHR does not provide a comprehensive definition of the notion of "national security" and mentions that this concept cannot be exhaustively defined.[1] However, its case-law shows that the concept of national security definitely includes the protection of state security and constitutional democracy from espionage, terrorism, support for terrorism, separatism and incitement to breach military discipline.[2]

On the other hand, the margin of appreciation doctrine is explicitly enshrined in the Preamble of the ECHR and is also deeply entrenched in the Court's jurisprudence. The doctrine reflects the principle of subsidiarity, recognizing that national authorities are better placed than an international court to assess local needs and circumstances. However, this discretion is not unlimited and goes hand in hand with the European Supervision.[3]

The margin of appreciation doctrine has fueled an ongoing debate and has given rise to different evaluations among legal scholars and practitioners. For example, Bosko Tripkovic, a senior lecturer of Birmingham Law School, applauds the development of the doctrine as far as it makes the ECHR more sensitive to national context and ensures that domestic understandings are taken into account when the Convention is interpreted and applied.[4] At the same time, this doctrine has attracted significant criticism. For example, Belgium jurist and former judge of the ECtHR, Jan De Meyer strongly opposed it. In his

---

[1] *Esbester v. the United Kingdom* [ECHR], No. 18601/91, [02-04-1993]. *Hewitt and Harman v. the United Kingdom* [ECHR], No. 20317/92, [01-09-1993].
[2] Council of Europe (2013). *National security and European case-law*, https://rm.coe.int/168067d214, 3.
[3] European Court of Human Rights (2012). Brighton Declaration – *High level conference on the future of the European Convention on Human Rights* [online], https://www.echr.coe.int/documents/d/echr/2012_brighton_finaldeclaration_eng, 3.
[4] TRIPKOVIC, Bosko (2022). A New Philosophy for the Margin of Appreciation and European Consensus. *Oxford Journal of Legal Studies*. 42, 207-234 [online]. https://academic.oup.com/ojls/article/42/1/207/6377894, 234.

partly dissenting opinion in "Z v. Finland" (1997), he stressed that "where human rights are concerned, there is no room for a margin of appreciation which would enable the States to decide what is acceptable and what is not". Even more, he called upon the Court "to banish that concept from its reasoning".[5] Judge Rozakis, another former judge of the ECtHR, also criticized the concept of the margin of appreciation in his concurring opinion in "EGELAND and HANSEID v. Norway" (2009), arguing its tendency to be applied automatically.[6] Timothy Jones has also expressed criticism of the margin of appreciation doctrine arguing that its use devaluates Convention rights at the expense of their limitations.[7]

It should be noted that the precise scope of the margin of appreciation depends on several factors, including the existence of a European consensus, the nature of the right involved, and the aim pursued by the impugned measure. These factors become especially complex in surveillance-related cases. For example, in Klass and Others v. Germany (1978) and Leander v. Sweden (1987), the ECtHR afforded states a relatively wider margin of appreciation because of their national security concerns. In contrast, in Roman Zakharov v. Russia (2015) and Big Brother Watch and Others v. the United Kingdom (2021), the Court applied stricter scrutiny, emphasizing the need for effective and sufficient safeguards against abuse and arbitrariness. Such varying interpretations give rise to questions about the predictability and consistency of the ECtHR's approach to surveillance-related cases. As Jan Kratochvíl correctly concludes, the Court lacks a clear systematic approach of the margin of appreciation and often does not say anything on the width of the margin explicitly, which makes this doctrine saw "much inconsistency and adhockery", an "eclectic case-by-case analysis" with no specific underlying theory.[8]

Defining the margin of appreciation has become even more challenging with technological advancements, especially, with the fast-evolving Artificial Intelligence (AI). It is not disputable that modern AI technologies have potential to be used for defense or national security purposes, while at the same time posing new and unforeseeable risks to fundamental human rights and freedoms, including the private life by means of enhanced

[5] *Z v Finland* [ECHR], No. 22009/93, [25-02-1997], partly dissenting opinion of judge De Meyer, III.
[6] EGELAND and HANSEID v. Norway [ECHR], No. 34438/04, [16-04-2009], concurring opinion of judge ROZAKIS, (a).
[7] MOWBRAY, J. Alastair (2007). Cases and Materials on the European Convention on Human Rights, United States. Second edition [online]. United States: Oxford University press. Google Books, 631.
[8] KRATOCHVIL, Jan (2011). The Inflation of the Margin of Appreciation by the European Court of Human Rights, *Netherlands Quarterly of Human Rights,* 29(3), 324-357 [online]. https://www.corteidh.or.cr/tablas/r26992.pdf, 347-351.

surveillance capabilities. These concerns have not been refused at the European Union level, which led to the adoption a 2024/1689 regulation that establishes common and harmonized rules for the use of AI.[9]

In the light of the foregoing, the present Master's thesis will examine the main factors influencing the breadth of the margin of appreciation afforded to national authorities in surveillance-related cases concerning the protection of national security. For this reason, the thesis also analyzes the key requirements that national legislation regulating surveillance measures must meet in relation to different types of surveillance, namely targeted and mass surveillance to avoid abuse and arbitrary use of surveillance measures in the name of national security.

Relevance of the topic. Balancing privacy and security remain one of the main challenges in a democratic society, especially in the digital world. Establishing clear limits for state surveillance is crucial to prevent abuse. The margin of appreciation plays a vital role in this process. Given that the doctrine is a context-based, it is highly important to examine how its interpretation has evolved over time in cases concerning protection of national security in a context of surveillance in order to determine whether the Court's existing jurisprudence adequately safeguards privacy while accommodating legitimate national security interests.

The aim. This Master's thesis aims to identify and analyze the key factors determining the scope of the margin of appreciation granted to national authorities in national-security-related surveillance cases within the jurisprudence of the ECtHR.

The objectives. To achieve the above-mentioned aim, the thesis examines the concept of national security, its main features and the scope of the right to privacy under Article 8 of the ECHR, including the conditions under which interferences within this right may be justified. It also distinguishes targeted and mass surveillance, identifies their characteristics and analyze the ECtHR's landmark judgements regarding both types of surveillance. The paper assesses the essence, development and purpose of the margin of appreciation doctrine as well as the principle of proportionality. It identifies and evaluates the key factors which

[9] Regulation No 2024/1689 of the European Parliament and of the Council of 13 June 2023 on laying down harmonized rule son artificial intelligence and amending regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). OJ L, 12.7.2024, pp. 2, 9, 12, 25.

influence the breadth of the margin of appreciation in national security related surveillance cases. The Master's thesis also suggests the main findings.

The object of this Master's thesis is the ECtHR's case-law concerning restrictions on the right to privacy on national security grounds in the context of surveillance.

Research methods. The present Master's thesis applies several research methods, including the comparative method, the linguistic (grammatical) method, and the systemic analysis method. These methods are used to examine the relevant case-law of the ECtHR. For this purpose, I will use the HUDOC database, which provides access to the Court's judgments, as well as the ECHR Knowledge Sharing platform (ECHR-KS), which contains case-law guides and thematic materials. Searches will be conducted by Article and with keywords such as surveillance, right to privacy, mass surveillance, bulk surveillance, national security. After collecting the relevant case-law, I will classify cases by time period and by type of surveillance measure and then compare how the Court's reasoning has evolved over time, with particular attention to its application of the margin of appreciation and the proportionality principle in earlier versus more recent surveillance cases.

Originality of the Master's thesis lies in its systematic and comparative approach to analyze how the ECtHR applies the margin of appreciation in relation to different types of surveillance, when states use them to protect their national security. By doing so, the research contributes to a deeper understanding of whether the ECtHR's case law offers a coherent and principled framework for protecting privacy in the face of evolving security threats and what challenges may be faced in future.

Sources. Given the main topic and aim of this Master's thesis, the most important sources used in this paper are the legal acts and official documents of the ECtHR and the Council of Europe on national security, surveillance measures and the scope of the margin of appreciation in this regard. The special literature, including books and scholarly articles, is also applied to the analysis each issue.

Among these sources, the 2013 Council of Europe report "National security and European case-law" is particularly important. Part I of this report is especially relevant, because it analyzes secret surveillance and Article 8 of the ECHR, including the scope of the State's margin of appreciation in national-security-related cases and discusses a wide range of landmark ECtHR judgements. Furthermore, the 2024 ECtHR factsheet on mass

surveillance, which chronologically overviews the Court's key cases and reasoning, is central as it outlines the development of the Court's approach to bulk interception regimes. Similarly, thematic insight is offered by the 2025 joint factsheet of the ECtHR and the European Union Agency for Fundamental Rights (FRA), which updates earlier materials. At the same time, the 2025 Council of Europe Guide on Article 8 of the ECHR constitutes an important source, as it systematically examines the right to privacy, including positive and negative obligations under this article and the Court's principles regarding secret surveillance. These publications, among others, were chosen because they present official and trustworthy interpretations of the ECtHR's approaches, summarize the relevance case-law as well as help to identify the general standards established by the ECtHR.

As for the scholarly literature, the 2020 online Article by Nóra Ní Loideain "The Approach of the European Court of Human Rights to the Interception of Communications", plays a special role in this thesis. This article critically analyzes the ECtHR's approach on secret surveillance in the context of national security and provides in-depth analysis of the Court's use of the margin of appreciation doctrine supported by the other scholars. Furthermore, Yutaka ARAY's 2001 book "the margin of appreciation doctrine and the Principe of proportionality in the jurisprudence of the ECHR as well as Steven GREER' book on "the Margin of Appreciation: Interpretation and Discretion under the European Convention on Human Rights" and Howard Charles YOUROW's book "The margin of appreciation doctrine in the dynamics of European Human Rights Jurisprudence" play an essential role in critically assessing and defining the key features and factors influencing the margin of appreciation's scope. What is more, the article by Ferenc KOPEC "National security as a legitimate excuse to human rights restrictions" contributes to examine national security as a ground for restricting human rights in general.

"In view of the risk that a system of secret surveillance set up to protect national security […] may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse".

- Grand Chamber of the ECtHR,
"Big Brother Watch and others v. the United Kingdom" (2021).

Chapter 1. Surveillance under national security ground in ECtHR jurisprudence

There is no universally accepted definition of national security. Its basic characteristics indicate that it is closely linked to State sovereignty and protection of democratic institutions, encompassing both internal and external dimensions of security. For example, the Court of Justice of the European Union (CJEU) in 2020 judgements "Privacy International v. Secretary of State for the Foreign and Commonwealth Affairs and Others" and "La Quadrature du Net and Others v. France" described national security as the sole and primary responsibility of each state. According to the CJEU "that responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilizing the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities".[10]

In parallel to international definitions, it is also important to examine national approaches to understanding national security, as these national perspectives show what each state consider necessary to safeguard against threats. States have the diversity in this regard.

For example, the Czech Republic identifies the main element of national security as the protection of sovereignty, territorial integrity, its democratic foundations, lives, health and property of its population. Germany defines national security primarily in terms of imminent danger to the free democratic order; sovereignty and territorial integrity of the State; the security of its institutions; and the integrity of the constitutional system. Hungary

[10] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters [GCHQ], Security Service [MI5], Secret Intelligence Service [MI6]* [CJEU], No. C-623/17, [15.10.2020], §74. *La Quadrature du Net and Others,* [CJEU], Nos. C-511/18, C-512/18 and C-520/18, [06.10.2020], §135.

considers national security to include the protection of state sovereignty and lawful order; territorial integrity; political, economic and military interests; the exercise of fundamental human rights and freedoms; multi-party democratic system; functioning of legal institutions as well as the protection of citizens against terrorism. As for the United Kingdom, it generally views national security as the security of the State and its people; the stability of its system of government; protection of democratic, legal and a constitutional structure, military defense capabilities; safeguarding to foreign relations; and the commitment to the peaceful coexistence of nations.

Although there is no single internationally or nationally acceptable definition of national security, the approaches of international and national authorities taken together, demonstrates that the concept of national security definitely involves the internal and external security of the state. At least, national security includes - the sovereignty of the State; the integrity of its territory, institutions and critical infrastructure; the protection of the democratic and lawful constitutional order as well as the protection of citizens and residents against serious threats to their lives, health and human rights.[11]

It should be noted that national security is recognized as one of the legitimate grounds for restricting certain non-absolute/qualified rights, including the right to privacy under Article 8 of the European Convention on Human Rights. While the ECtHR recognizes that national authorities enjoy a fairly wide margin of appreciation in assessing what constitutes a threat to national security and in choosing the means to protect it, this discretion cannot be stretched beyond the natural meaning of this concept. This means that national authorities still remain subject to European Supervision, which ensures that they act within the limits of their margin of appreciation when protecting national security.[12] In the name of protecting national security, states often use different types of surveillance measures. As a former Vice-President of the European Commission Viviene Reding has stated, the concept of national security does not mean that "anything goes": States do not enjoy an unlimited right of secret surveillance.[13] Accordingly, such measures remain subject to

[11] Council of Bars & Law Societies of Europe (2019). CCBE recommendations on the protection of fundamental rights in the context of "national security" [online], https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf, 17.

[12] *C.G. and Others v. Bulgaria* [ECHR], No. 1365/07, [24-04-2008], §43.

[13] BIGO, Didier. CARRERA, Sergio. HERNANZ, Nicholas. JEANDESBOZ, Julien. PARKIN, Joanna. RAGAZZI, Francesco. SCHERRER, Amandine (2013). Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law. *CEPS Paper in Liberty and Security in Europe*, 61, 1-60 [online].

judicial scrutiny by the ECtHR to ensure that legal standards developed in the Court's case-law are met.

For this reason, this Chapter provides a general overview of the scope of the right to privacy under Article 8 of the ECHR, positive and negative obligations under this article as well as the conditions under which interferences with the right to privacy may be considered justified on national security grounds in the context of surveillance.

1.1. The structure and scope of Article 8 of the Europan Convention on Human Rights

The European Convention on Human Rights has been described as a "constitutional instrument of European public order" in the field of human rights.[14] It was adopted in 1950 by the Council of Europe in response to the widespread and systematic human rights violations witnessed in Europe during the Second World War. Accordingly, the ECHR was primarily intended to serve as an alarm bell to other West European States, urging them to take action against serious human rights violations.[15] The ECHR entered into force in 1953 and has been ratified by all 47 member states of the Council of Europe. By doing so, the high contracting parties have undertaken the obligation to respect and secure for everyone within their jurisdiction the rights and fundamental freedoms guaranteed by the ECHR.[16]

The Convention sets out a catalog of civil and political rights which are essential for the proper functioning of a democratic society. Among these rights, the right to privacy holds a particular significance. The right to privacy is widely recognized as a universal human right and is explicitly protected by several other international instruments, including Article 12 of the Universal Declaration of Human Rights (UDHR),[17] Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[18] and Article 7 of the EU Charter of Fundamental Rights.[19] As U.S. Supreme Court Justice Louis Brandeis defined,

---

https://cdn.ceps.eu/wpcontent/uploads/2013/11/No%2062%20Surveillance%20of%20Personal%20Data%20by%20EU%20MSs.pdf, 24.

[14] *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [ECHR], No. 45036/98, [30-06-2005]. *N.D. and N.T. v. Spain* [ECHR], Nos. 8675/15 and 8697/15, [13-02-2020].

[15] HARRIS, David John; O'BOYLE, Michael; BATES, Ed and etc. (2023). *Law of the European Convention on Human Rights*. Fifth edition [online]. Oxford: Oxford University Press. Google Books, 3.

[16] MURRAY, John L (2011). The Influence of the European Convention on Fundamental Rights on Community Law. *Fordham International Law Journal*, 33, 1388-1422 [Online]. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2208&context=ilj&httpsredir=1&referer=, 1403.

[17] Universal Declaration of Human Rights (1948). United Nations. *Official website of the United Nations*.

[18] International Covenant on Civil and Political Rights (1966). United Nations. *Official website of the United Nations*.

[19] Charter of Fundamental Rights of the European Union (2000). European Union. *Official Journal of the European Communities*, 2000, C 364/1.

the right to privacy is "the most comprehensive of rights and the right most valued by civilized men".[20]

However, it should be noted that there is no universally accepted definition of the term "privacy". Scholars have offered various interpretations of this concept. For example, Thomas Cooley defined privacy as "the right to be let alone".[21] Another scholar, Ruth Gavison argued that privacy encompasses anonymity, solitude and secrecy,[22] while Helen Nissenbaum emphasizes the importance of privacy in the context of personal data protection.[23] Despite different approaches, there is no doubt that the notion of privacy covers a wide range of personal life aspects, including freedom from unlawful surveillance.

The ECHR is no exception in this recognizing the importance of privacy. Notably, Article 8 of the Convention guarantees the right to respect for private and family life. According to Article 8(1) "Everyone has the right to respect for his private and family life, his home and his correspondence". However, this right is not absolute and may be subject to restrictions under Article 8(2), which states that: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[24]

As the text indicates, Article 8 of the ECHR covers the four interrelated interests: private life; family life, home and correspondence. However, none of these concepts is defined in the ECHR itself. Instead, each has an autonomous meaning in the ECtHR's case-law. For example, generally, the ECtHR has established that the concept of "home" refers to "the place, the physically defined area, where private and family life develops"[25], while

[20] The U.S. Supreme Court. Decision of 4 June 1928 in a criminal case Nos. 493, 532 and 533.
[21] COOLEY, Thomas M (1888). *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract.* Second edition [online]. Chicago: Callaghan & Company. Google Books, 29.
[22] GAVISON, Ruth (1980). Privacy and the Limits of Law. *The Yale Law Journal*. 89, 421-471 [online]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957, 428.
[23] NISSENBAUM, Helen (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life* [online]. Standford, California: Stanford University Press. Google Books.
[24] European Convention on Human Rights (1950). Council of Europe. *Official website of the Council of Europe*.
[25] *Giacomeli v. Italy* [ECHR], No. 59909/00, [02-11-2006].

the notion of “correspondence” protects private communications/conversations regardless of their form and content.[26]

It is important to note that the scope of Article 8 is not limited to these above-mentioned four interests. The ECtHR has interpreted this provision much broadly. In particular, in “Niemietz v. Germany” (1992) it held that “the Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life".[27] However, the Court also mentioned that it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings”.[28] This definition clarifies that the scope of Article 8 includes any place where an individual’s interaction with others is affected.[29]

The high contracting parties have both negative and positive obligations to protect rights guaranteed by Article 8 of the ECHR. The negative obligation requires public authorities to refrain from arbitrary interference with an individual’s private and family life, home and correspondence.[30] On the other hand, the positive obligation, which is also inherent for the realization of the right to privacy, requires states to take effective steps to ensure respect for these rights. The positive obligations include, among others, adopting legislative or administrative measures and in serious cases, even implementing criminal-law mechanisms to offer adequate protection.[31]

[26] *Halford v. The United Kingdom* [ECHR], No. 20605/92, [25-06-1997].
[27] *Niemietz v. Germany* [ECHR], No. 13710/88, [16-12-1992], §29.
[28] Ibid.
[29]HARRIS, David John; O’BOYLE, Michael; BATES, Ed and etc. (2023). *Law of the European Convention on Human Rights*. Fifth edition [online]. Oxford: Oxford University Press. Google Books, 504.
[30] *Drelon v. France* [ECHR], Nos. 3153/16 and 27758/18, [08-09-2022]. *Kroon and Others v. the Netherlands* [ECHR], No. 18535/91, [27-10-1994].
[31] *Bédat v. Switzerland* [ECHR], No. 56925/08, [29-03-2016].

1.2. Justifiable interferences with the Right to Privacy under Article 8(2) of the European Convention on Human Rights

In most surveillance-related cases the central question is not how intrusive the relevant surveillance measure is, regardless of whether it pursues national security or other legitimate aims, but whether it can be justified under Article 8(2).[32] Therefore, examining Article 8(2) of the ECHR and its main requirements is especially important for the subject matter of the present thesis.

As previously mentioned, the rights guaranteed by Article 8(1) are not absolute, which means that state authorities may interference with these rights, but only if such restriction meets the three cumulative conditions set out in Article 8(2). This provision requires that: 1. any interference must be "in accordance with the law"; 2. It must pursue one or more legitimate aims listed in Article 8(2); and 3. It must be "necessary in a democratic society" in order to achieve any such aim.[33] This three-part test is well-established in the case-law of the ECtHR and is applied to assess whether limitations on non-absolute right(s), such as the right to privacy, are justified. For clarity, briefly review each criterion of this test.

Generally, the first requirement that any interference must be "in accordance with the law" means that the impugned measure must have a legal basis in national legislation and must also meet quality of law standard. In particular, the domestic law must be clear, adequately accessible and foreseeable to its effects.[34] However, it should be emphasized that the criterion of "foreseeability" in surveillance-related cases is not the same as in other areas. Given the special nature of secret surveillance, the ECtHR has acknowledged that individuals cannot be expected to foresee when the authorities might use secret surveillance and adjust their conduct accordingly.[35] This interpretation should be considered justified because requiring such level of foreseeability would undermine the very essence of secret surveillance, which is intended to be conducted without knowledge of the public at large.

[32] LOIDEAIN, Ni Nora (2020). The approach of the European Court of Human Rights to the interception of communications. EU Data Privacy Law and Serious Crime (Oxford University Press), *Oxford Data Protection & Privacy Law Series*, 30-73 [online], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699386, 44.
[33] *Kennedy v. the United Kingdom* [ECHR], No. 26839/05, [18-05-2010].
[34] *Rotaru v. Romania* [ECHR], No. 28341/95, [04-05-2000]. *S. and Marper v. the United Kingdom* [ECHR], Nos. 30562/04 and 30566/04, [04-12-2008].
[35] *Roman Zakharov v. Russia* [ECHR], No. 47143/06, [04-12-2015].

However, it does not mean that the national laws regulating secret surveillance regimes are exempt from legal requirements. Instead, the ECtHR has explicitly emphasized the need for clear and detailed rules governing the use of such measures. Particularly, the ECtHR requires that the contested domestic law must be sufficiently clear to give individuals an adequate indication of the conditions and circumstances under which secret surveillance may be authorized and conducted. The law must also indicate the scope of discretion exercised by the competent public authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[36]

The second criterion of the three-part test requires that an impugned measure must pursue one or more of legitimate aims. These includes national security; public safety; the economic well-being of the country; prevention of disorder or crime; the protection of health or morals; the protection of the rights and freedoms of others. Accordingly, national security is explicitly listed in Article 8 of the ECHR as one of the legitimate grounds that may justify interference with the right to privacy.

As for the third criterion of the three-part test that an impugned measure must be necessary in a democratic society, it means that any interference must correspond to a pressing social need, and be proportionate to the legitimate aim pursued. In addition, state authorities must provide relevant and sufficient reasons to justify an interference. The necessity criterion primarily concerns whether the respondent government has struck a fair balance between an individual's right to privacy and state's public interest to protect their national security, including in the context of mass surveillance.[37] This is the stage when the doctrine of margin of appreciation becomes especially relevant.

[36] *Malone v. the United Kingdom* [ECHR], No. 8691/79, [02-08-1984]. *Leander v. Sweden* [ECHR], No. 9248/81, [26-03-1987]. *Huvig v. France* [ECHR], No. 11105/84, [24-04-1990].
[37] ÇALI, Başak (2018). Balancing Test: European Court of Human Rights (ECtHR). Oxford Public International Law [online]. https://opil.ouplaw.com/display/10.1093/law-mpeipro/e3426.013.3426/law-mpeipro-e3426, 26

Chapter 2. Types of surveillance – targeted and mass (bulk) surveillance

First of all, it should be mentioned that the term "surveillance" is not a new concept. However, in today's digitized world, the practice of secret surveillance has become more widespread and technologically advanced. These measures and their rapid developments raise serious concerns in regard to the right to privacy.

The ECtHR has developed a rich case-law in the field of secret surveillance. These cases differ from each other in terms of the types of surveillance measures used, the time period involved, the arguments provided by respondent governments as well as the nature of the national security threats. However, the central issue in all surveillance-related cases remains the same: whether the respondent state acted within the margin of appreciation grantedd to them and has struck a fair balance between national security interest and the right to privacy and how the ECtHR assesses it.

For a better understanding of the above-mentioned issues, it is essential to clarify what is meant by surveillance. In this regard, it should be mentioned that the term „secret surveillance" refers to measures such as the observation and recording of an individual's movements, the use of hidden listening devices, the interception of communications and other actions which invade a person's private sphere.[38] Not all the types of surveillance have been assessed by the ECtHR, which is unsuprinig given the rapid evolution of surveillance techniques in the digital era. However, according to the ECtHR's case-law, two main categories of surveillance can be disingushed. These are targeted surveillance and mass (bulk) surveillance.[39]

2.1. Targeted and mass surveillance: definitions and characteristics

To begin with, the main essence of the notion of the targeted surveillance is that it refers to the covert collection of conversations, telecommunications, movements and metadata of specifically identified individuals or groups. One of the main characteristics of the targeted surveillance measures is that they are conducted with a reasonable suspicion that the target is involved in criminal activities. Such activities may involve planning, committing or having committed crimes or other acts that may justify conducting of secret surveillance, including activities that may endanger national security. Targeted surveillance is primarily

[38]HARRIS, David John; O'BOYLE, Michael; BATES, Ed and etc. (2023). *Law of the European Convention on Human Rights*. Fifth edition [online]. Oxford: Oxford University Press. Google Books, 555.
[39] European Commission for Democracy Through Law (Venice Commission) (13-12-2024). *Report on a rule of law and human rights compliant regulation of spyware* [online]. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)043-e.

used in the investigation of criminal activities. One of its main defining characteristics is that it has a clearly identified subject, in other words, such surveillance measures have a targeted individuals or groups of individuals. [40]

In contrast to targeted surveillance, mass (bulk) surveillance is not necessarily directed at specific individuals or groups. Rather, it is proactive in nature and aims to identify previously unknown threats rather than investigating known ones. Hence, mass surveillance does not require prior suspicion against particular persons.[41] What is more, mass surveillance may target not only the content of electronic communications, but also related metadata, such as subscribers' personal information, traffic and location data. According to the ECtHR, this metadata can be equally intrusive because they can offer a detailed picture of an individual's private life, including their habits, permanent or temporary places of residence, daily movements, activities as well as their personal and social relationships with others.[42]

More importantly, the privacy risks associated with mass surveillance are not limited only to the above-mentioned activities. Such regimes may also involve attempts to decrypt encrypted communications. It is also worth mentioning that mass surveillance systems often function by bulk interception, which entails the access and storage of large volumes of data transmitted through the internet infrastructure.[43] States may also require electronic communication service providers to retain and store users' communications and related metadata.[44] These definitions make it clear that mass surveillance regimes enable governments to access a large volume of data either directly or indirectly, via targeted mechanisms.

[40] Council of Europe (2018). *Mass Surveillance* [online]. https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e.
[41] Ibid.
[42] Big Brother Watch and Others v. The United Kingdom [ECHR], Nos. 58170/13 62322/14 and 24960/15, [25.05.2021].
[43] The European Court of Human Rights ("ECtHR") and the European Union Agency for Fundamental Rights (28-02-2025). *Mass surveillance – ECtHR and CJEU Case-law* [online]. https://fra.europa.eu/sites/default/files/fra_uploads/ecthr-fra-2025-mass-surveillance_en.pdf.
[44] Ibid.

2.2.ECtHR case-law on targeted and mass surveillance

This subchapter provides an overview of the main ECtHR judgements on both targeted and mass (bulk) surveillance. It examines the factual circumstances in which states interfered with applicants' right to privacy on national security ground, the Court's key findings and reasoning, legal standards established and applied in each case by it.

2.2.1. Targeted surveillance cases

The following subsection examines the key ECtHR cases on targeted surveillance, that is measures directed at specific individuals or identifiable group of individuals, normally, in the context of criminal investigation. The Court has developed six minimum safeguards (also known as the Weber safeguards) to assess the Convention compliance of targeted surveillance with Article 8 of the ECHR. These safeguards will be explained and applied to the cases discussed below. Also, each judgement will be followed by a brief explanation about its importance. Cases are presented chronologically to illustrate the development of the Court's approach evolving time.

2.2.1.1. Klass and Others v. Germany (1978)[45]

Klass and Others v. Germany is an early case on targeted surveillance. it concerns the compatibility of domestic law governing secret surveillance, namely the Basic Law and the G 10 Act of the Federal Republic of Germany, with Article 8 of the Convention.

In this case, five German nationals challenged the legislation, which allowed authorities to open and inspect mail and post, read telegraphic messages as well as to listen and record telephone conversations. The applicants did not dispute State's authority to conduct surveillance in general. Instead, they argued that the domestic legislation lacked sufficient guarantees against abuse. In particular, they argued that the contested legislation it did not impose an obligation to notify persons after surveillance and there was not an available effective judicial remedy against the ordering and/or execution of such measures. Accordingly, they claimed that the legislation in question violated Article 8 of the Convention.

[45] *Klass and Others v. Germany* [ECHR], No. 5029/71, [06.09.1978].

The Court first found that the contested legislation interfered with the applicants' right to respect for private and family life and correspondence as guaranteed under Article 8 of the ECHR. The central issue was whether such interference was justified under paragraph 2 of Article 8, as the Court stressed secret surveillance can be tolerated only when it is strictly necessary for safeguarding the democratic institutions and processes.

Applying the three-part test under Article 8(2), the Court found that the first two requirements were fulfilled as the impugned measures were prescribed by national law and pursued legitimate aims of protecting national security and preventing disorder or crime. As to the necessity of the interference, the Court acknowledged that given the rapid technological advancements, states face highly sophisticated threats such as espionage and terrorism. Hence, national authorities have *a certain discretion* to operate surveillance measures to protect their national security from such threats under certain circumstances. However, such surveillance must be accompanied by adequate and sufficient guarantees against abuse and arbitrariness. The Court added that in assessing the safeguards, it takes into account, among others things, the nature, scope and duration of the surveillance, the grounds for authorization, the competent authorities involved in permitting, conducting and supervising such measures as well as the availability of effective remedies.

In the present case, the Court found that the German G 10 Act set strict conditions regarding surveillance. In particular, according to this legal Act, surveillance measures could be ordered only when factual circumstances indicated serious criminal activity and when other means were deemed ineffective. Surveillance measures were only applied to specific people - suspected individual(s) or presumed contacts. What is more, internal administrative procedure existed regarding the destruction of obtained materials, the maximum duration of the surveillance, and the discontinuation of measures. All these safeguards were considered effective by the ECtHR to prevent abuse.

It is interesting that despite the above-mentioned guarantees, the Court could not overlook the fact that under domestic legislation judicial control on surveillance was excluded. Instead, supervision was exercised by an official qualified for judicial office at initial stage and then by two independent bodies - the Parliamentary Board and the G 10 Commission. Although, judicial review would be desirable, the Court regarded that the mentioned supervisory mechanisms provided sufficient protection. Similarly, while there was no automatic notification requirement in every case, the Court was satisfied that under German law a person should be notified about surveillance as soon as that could be done

without jeopardizing its purpose. Decision whether an individual concerned should be notified was made by an independent the G10 Commission, ensuring balance between notification mechanism and the need for protecting secrecy when necessary. Overall, the Court considered that the German legislation provided sufficient and effective safeguards for secret surveillance. Accordingly, it found no violation of Article 8 of the Convention.

Several important aspects can be identified in this case. First, as early as 1978, the Court already acknowledged the rapid technological developments and the sophisticated threats they can pose to states' national security. For this reason, the Court granted certain discretion to national authorities to address such threats, including by means of secret surveillance measures. On the other hand, the Court recognizes the inherent risk of abuse in secret surveillance and requires sufficient guarantees. In this regard it is important to note, that even non-judicial review was considered acceptable, if the relevant body meets the requirements of independency and impartiality. Similarly, the absence of obligatory notification mechanism did not automatically constitute a violation of Article 8, as the Court assessed the secret surveillance system as a whole and the potential effects of any shortcoming.

2.2.1.2. Weber and Saravia v. Germany (2006)[46]

The present case concerned the compatibility of several provisions of the G 10 Act of Federal Republic of Germany, as amended in 1994, with Article 8 of the ECHR. As a result of these amendments, the powers of the Federal Intelligence Service were expanded and included recording of telecommunications through so-called strategic monitoring as well as the use and transmission of obtained personal data to other authorities. Under domestic law, strategic monitoring referred to the interception of telecommunications to identify and prevent serious threats to Germany, such as armed attacks, international terrorism and other serious offences. The applicants claimed that these provisions violated their right to respect for private life and correspondence as guaranteed by Article 8 of the Convention.

The Cout first found that the contested provisions interfered with the applicants' rights under Article 8 for several reasons. Notably, it held that the mere existence of legislation permitting secret monitoring creates a threat of surveillance for any individuals covered by the law, regardless of they were actually monitored. In addition, the transmission and use

[46] *Weber and Saravia v. Germany* [ECHR], No. 54934/00, [29.06.2006].

of personal data by authorities constituted separate interferences. Provisions allowing the destruction of collected data and refusal to notify individuals concerned were also additional interferences.

The Court then assessed whether the interference was justifiable under Article 8 (2) by applying the three-part test. The Court held that the interference was prescribed by national law, which satisfied the quality of law criteria and contained minimum safeguards against arbitrary interference. In particular, the impugned provisions enumerated the exact offences that could give rise to an interception order, indicated categories of persons allegedly subject to monitoring, limited the duration of telephone tapping and detailed the procedures for transmitting and destroying data. The second criterion was also satisfied, as far as the interference pursued legitimate aims of protecting national security and preventing crime.

As to the necessity, the Court acknowledged that national authorities enjoy *a fairly wide margin of appreciation* in choosing the means to protect their national security. However, the ECtHR also emphasized that such surveillance must be accompanied by adequate and effective guarantees against abuse. The Court assessed the proportionality of each impugned measure separately.

Firstly, in relation to strategic monitoring, the Court noted that the amended G 10 Act significantly broadened the range of subjects for monitoring but at the same time it was accompanied by sufficient safeguards. These guarantees included detailed and strict rules for implementing surveillance measures, processing, storing and destroying of obtained data, supervision by two independent bodies, as in Klass and Others v. Germany.

Regarding the transmission and use of data obtained, the Court found that it was allowed only when necessary for strategic monitoring, related to serious criminal offences and based on facts rather than mere indications. Procedures for data destruction and post-surveillance notification were also considered adequate, as persons concerned should be notified as soon as possible without jeopardizing the purpose of the monitoring.

In the light of the foregoing, Court held that Germany acted within its margin of appreciation and did not overstep it, because the contested legislation ensured adequate and effective guarantees against abuses of the State's strategic monitoring. Such guarantees were independent supervision, clear limits on use and transmission of data as well as rules on data destruction and notification.

According to the above-mentioned, the Court declared the application inadmissible.

This case demonstrates the importance of the quality of domestic law governing secret surveillance regimes. It show that the expansion of national authorities' powers in strategic monitoring and the processing of personal data does not automatically violate Article 8 of the ECHR, if national law includes adequate and sufficient safeguards against abuse.

The present case should be distinguished from „Liberty and Others v. the United Kingdom"(2008). Their comparison is interesting because Liberty and Others likewise concerned the interception and examination of external communications and as in Weber, the interference had a legal basis in domestic legislation, namely the interference was prescribed by the Interception of Communications Act 1985 (ICA) and the Regulation of Investigatory Powers Act 2000 (RIPA). However, the main difference between these two cases is the quality of domestic law. In contrast to Weber, the Court held in Liberty that the UK legislation did not satisfy the requirements of the accesibility and foreesibility, particularly in relation to the procedures for selecting, examination, sharing, storing and destroying intercepted material. As a result, the Court found in Liberty and Others case that the contested legislation did not provide sufficient guarantees against abuse.

Notably, the Court found that the UK authorities enjoyed an extremely broad and even unfettered discretion in authorizing the interception of external communications. Another important shortcoming was the lack of public accessibility of the "arrangements" governing surveillance, as they were set out in internal rules and instructions. This deficiency was not counterbalanced by the oversight mechanism, as far as the supervisory body was not permitted to disclose the content of the arrangements to the public. Consequently, procedures for the examination, use, and retention of intercepted material were not available to public scrutiny.[47]

Accordingly, the ECtHR found a violation of Article 8 of the Convention. The comparison between these two cases makes it clear that even interception have a legal basis in national legislation, the decisive factor is the quality of the contested law and whether it contains sufficient and adequate safeguards against abuse and arbitrariness.[48]

[47] *Liberty and Others v. the United Kingdom* [ECHR], No. 58243/00, [01-07-2008]. §§64-68.
[48] *Liberty and Others v. the United Kingdom* [ECHR], No. 58243/00, [01-07-2008]. §§69-70.

2.2.1.3. Roman Zakharov v. Russia (2015)[49]

The applicant was the editor-in-chief of a publishing company and the chairperson of a non-governmental organization (NGO), which monitored media freedom in the Russian regions. He complained that the Russian system of the covert interception of mobile telephone communications violated his rights under Article 8 of the Convention. In particular, under the relevant domestic law, mobile network operators were required to install equipment, which permitted the Federal Security Service (FSB) to intercept all communications without prior judicial authorization.

One of the central issues in the present case was the applicant's victim status in the context of admissibility of the individual application as the applicant challenged the mere existence of legislation permitting secret surveillance. He was not affected by the contested legislation. In this regard, the Court reiterated that normally the Convention does not allow *actio popularis* and *in abstracto* complaints and that an applicant must demonstrate that impugned measures have directly affected his or her Convention rights. However, given the specific nature of secret surveillance, the Court permits general challenges under certain circumstances. In its early case-law, two parallel approaches were developed regarding this issue. In Zakharov, the Court considered it necessary to harmonize these approaches in order to prevent abusive interpretation and ensure foreseeability and clarity in this regard. Therefore, in the present case, the Grand Chamber adopted a uniform approach and established two criteria for general challenges. The first criterion is the scope of the legislation permitting secret surveillance measures. At this stage it should be determined, whether the legislation in question could affect the applicant either because he is a part of a targeted group or because the legislation affects all users of communication services. The second criterion refers to the availability of effective remedies at national level to challenge potential surveillance. Given that the Russian law directly affected all mobile telephone users and at the same time did not provide effective remedies at national level, the Court found that the mere existence of the contested law interfered with Article 8 of the Convention and the application should be considered admissible.

[49] *Roman Zakharov v. Russia* [ECHR], No. 47143/06, [04.12.2015].

Then, The Court assessed whether the interference was justified under Article 8(2). In this regard, it found that the interference had a legal basis at national legislation and pursued several legitimate aims, namely, protecting national security, economic well-being of the country and public safety as well as preventing crime. It then examined the quality of law, including its accessibility, foreseeability and necessity of the interference.

First, the Court listed the six minimum safeguards developed in its case-law on targeted secret surveillance, which must be set in national law to prevent abuse. These are the following: 1. the nature of offences which may give rise to an interception order; 2. a definition of the categories of people liable to have their communities intercepted; 3. a limit on the duration of interception; 4. the procedure to be followed for examining, using and storing the data obtained; 5. the precautions to be taken when communicating the data to other parties; and 6. the circumstances in which recordings may or must be erased or destroyed. The Court applied these general standards to the present case and identified several shortcomings regarding them, which are explained below.

The Court found that one of the legal acts governing interceptions, namely, Order no. 70 was never fully accessible to the public. Additionally, while Russian law indicated categories of criminal offences which might justify interception, its scope was very broad and included even minor ones. The contested legislation also did not clarify which person could be subject to surveillance. Similarly, it did not specify circumstances under which communications could be intercepted to protect Russia's national, military, economic or ecological security. Such regulation granted national authorities excessive discretion.

Regarding duration and data governing, the legislation indicated the periods for which warrants should be issued as well as the conditions for a warrant renew. However, it lacked clear rules for discontinuation of surveillance. Although clear procedures existed for storing, accessing, examining, using, communicating and destroying the intercepted data, the law allowed retention of clearly irrelevant data and granted a judge unlimited discretion about storing or destruction of obtained data after a trial.

Authorization procedure was also inadequate in the present case. Notably, while interceptions were authorized by the court, judicial scrutiny was limited in scope, as judges had not access to all relevant materials, which undermined their ability to assess the necessity and proportionality of the interception. This meant that the national legislation

granted law enforcement authorities almost unlimited discretion regarding the content of interception authorisations and the application of non-judicial urgent procedure.

Another shortcoming was also important. This deficiency was that law enforcement agencies had a direct access to all mobile communications and related data without judicial authorization. Moreover, supervision mechanisms were ineffective as far as interception records were not logged and recorded. Such practice made it impossible to detect any unlawful interception. Judicial supervision was also limited only to the initial authorisation stage. Subsequent oversight was exercised by executive authorities, which lacked independence and public scrutiny. The absence of two interrelated guarantees such as requirement to notify the person concerned and availability of effective remedies further undermined protection, as victim could not challenge interceptions in practice.

In the light of these shortcomings, the Court found that the Russian legislation on secret surveillance did not provide adequate and sufficient guarantees against abuse. Accordingly, the Court held that there had been a violation of Article 8.

As Nóra Ní Loideain correctly notes, Zakharov was the first case in which the ECtHR addressed a surveillance framework, which obliged communication service providers to structure their networks in a way that enabled Russian authorities to obtain real-time access to the content of the costumers' mobile communications as well as their location information.[50] This case is of particular significance for several other reasons. First, the Grand Chamber established a harmonized approach to victim status in secret surveillance cases, enabling individuals to challenge the Convention compliance of domestic surveillance legislation *in abstracto* even they were not personally affected. As a result, it has become clear under what circumstances individuals can lodge an individual application before the Court. Another key finding is that, the Court examined not only the text of the Russian legislation, which was overly broad and granted national authorities excessive power, but also its practical application. For example, it found that the mere existence of prior judicial authorization was insufficient, because it lacked practical effect. This means that even if secret surveillance system is formally regulated by law, this fact is not enough. Instead, states must ensure that these safeguards apply effectively in practice and are not only theoretical and illusory. For these reasons, this judgment provides important guidance

[50] LOIDEAIN, Ni Nora (2020). The approach of the European Court of Human Rights to the interception of communications. EU Data Privacy Law and Serious Crime (Oxford University Press), *Oxford Data Protection & Privacy Law Series*, 30-73 [online], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699386, 30.

for States on how to design and operate surveillance regimes and avoid excessive discretionary powers.

2.2.2. Mass (bulk) surveillance cases

This subsection examines the key ECtHR cases on mass (bulk) surveillance. This topic received particular attention after Edward Snowden's revelations, which showed the extensive power of national intelligence agencies in gathering a large amount of data by using advanced science and technologies.[51] As the Court noted itself in its comparative analysis, at least seven Contracting States officially operate bulk interception regimes, while at least thirty-nine Contracting States' legal framework enable cooperation in intelligence sharing.[52] Accordingly, these cases are of particular importance, as the Court stressed the inherent risks posed by mass surveillance and updated the six minimum safeguards developed on targeted surveillance.

2.2.2.1. Szabó and Vissy v. Hungary (2016)[53]

In the present case, the applicants complained that the Hungarian legislation on secret surveillance lacked sufficient guarantees against abuse and violated their right to respect for their homes, communications and privacy under Article 8 of the Convention.

According to the factual circumstances of the case, in 2011, Hungary adopted an anti-terrorism law, which empowered an Anti-Terrorism Task Force ("TEK") to conduct certain secret surveillance measures. These included secret searches and surveillance of houses, opening of letters and parcels as well as monitoring and recording of electronic communications or computer data transmission. Goven the nature of secret surveillance, these measures were conducted without the prior consent of the persons concerned and could be authorized for preventing and addressing to terrorist acts in Hungary as well as for rescuing Hungarians in distress abroad.

[51] Europea Parliament (2015). Mass Surveillance, Part 1 – Risks, Opportunities and Mitigation Strategies, https://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN1)_EN.pdf, 95.
[52] *Big Brother Watch and Others v. The United Kingdom* [ECHR], Nos. 58170/13 62322/14 and 24960/15, [25.05.2021].
[53] *Szabó and Vissy v. Hungary* [ECHR], no. 37138/14, [12.01.2016].

While accessing the case, the Court first noted that these measures interfered with the rights under Article 8 of the Convention and stressed that technological progress, which made sophisticated forms of surveillance technologies, required higher degree of protection for the right to privacy, including clear and detailed rules on interception.

Applying the three-part test under Article 8, the Court found that the impugned measures pursued legitimate aims of protecting national security and preventing disorder and crime. As to the necessity of the interference, the Court reiterated that any secret surveillance system must include adequate and effective guarantees against abuse. In this regard, national authorities, who are granted *a certain margin of appreciation* in choosing the means to protect their national security, they must strike a fair balance between national security and individual privacy.

The Court found that the Hungarian legislation failed to provide sufficient safeguards for several reasons. Firstly, it did not specify the categories of persons subject to interception. Instead, the law in question used overly broad and vague terms such as "persons concerned identified ... as a range of persons", enabling unlimited surveillance of a large number of citizens without requiring a link to terrorist threat. Such provision allowed that any person in Hungary could be subjected to such surveillance.

The absence of judicial supervision was also one of central issues in the present case. The authorization was granted by the Minister of Justice, which was a political actor and part of executive power. Hence, the Minister of Justice lacked independence and impartiality. The Hungarian law also did not provide neither post-judicial review nor mandatory notification mechanism for persons, who subjected surveillance.

It is of particular importance that in this case, the Court recognized the necessity of modern surveillance to fight against terrorism. At the same time, the Court also stressed that such technologies pose serious risks to peoples' private life and their reasonable expectations of privacy. Hence, the Court required from states that efforts to combat terrorism must not create a new threat of unfettered executive power intruding into citizens' private spheres through uncontrolled surveillance. In contrast to these requirements, the Hungarian legislation allowed mass surveillance, which raised serious concerns and the safeguards developed in earlier case law were no longer sufficient. As the Court noted the earlier safeguards must be strengthened to address modern large-scale surveillance.

Given the broad scope of the contested law, executive control over authorization, lack of independent review and the absence of notification requirement, the Court found that the Hungarian legislation lacked sufficient guarantees against abuse.

Accordingly, the Court found that there had been a violation of Article 8.

This case demonstrates that even terrorism-related threats cannot automatically justify the operation of secret surveillance system, if it is not accompanied by sufficient and adequate safeguards. Notably, the Court emphasized the heightened risks to the right to privacy posed by mass surveillance and acknowledged that such systems require a different approach compared to targeted interception. However, the Court did not introduce new safeguards designed exclusively for mass surveillance regimes and only mentioned such need.

2.2.2.2. Centrum för rättvisa v. Sweden (2021)[54]

The applicant, a non-governmental organization, claimed that the Swedish legislation and practice on bulk interception of communications violated Article 8 of the Convention.

First, the Grand Chamber examined the victim status, as the applicant challenged the legislation itself without demonstrating that it was directly subjected to secret surveillance. The Court held that the contested legislation should be examined *in abstracto*, as it potentially affected all individuals' telephone and internet communications and related data and there were not effective remedies for individuals, who suspected that they had been subjected to secret surveillance measures.

The Court stressed that assessing compliance of such regimes with the Convention has become especially difficult in the digital era, as most communications have now taken digital form and transmitted through global networks. While recognizing mass surveillance as a valuable technological capacity for protecting national security, the Court emphasized the need for adequate safeguards to prevent abuse and arbitrariness.

The Grand Chamber identified four stages in bulk interception: 1. Interception and initial retention of communications and related data – at this stage, electronic communications are intercepted in bulk and covers a large number of people, including those who are irrelevant for intelligence services; 2. Application of selectors to identify

[54] Centrum för rättvisa v. Sweden [ECHR], No. 25252/08, [25-05-2021].

relevant communications and related data – at this stage initial searching is conducted by applying selectors; 3. Examination of selected communications and related data by analysts; and, 4. Retention, use and sharing of the intercept material. As the Court defined, Article 8 applies to all these stages and the degree of interference with Article 8 rights increases in parallel to the bulk interception process progress.

It should be emphasized that the Court noted that the six minimum safeguards developed for targeted surveillance, so called the Weber safeguards, required adaptation to the specific features of bulk interception. The Court held that "While Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for these purposes, in operating such a system *the margin of appreciation afforded to them must be narrower* and a number of safeguards will have to be present".[55]

The Court clarified that the first two of the six "minimum safeguards" concerning specific offences or categories of people do not apply to bulk interception, as it is not conducted for criminal investigations. Instead, national law must clearly define the grounds for authorization of bulk interception and the circumstances in which communications may be intercepted. The remaining four safeguards are equally applicable to bulk interception.

One of the new safeguards concerns the "end-to-end safeguards". The latter guarantee requires the continuous assessment of necessity and proportionality, independent authorization, supervision as well as ex antre and post facto review. Independent authorizing body must be informed about the purpose of bulk interception and the bearers or communication routes to be intercepted. Another important safeguard is the existence of an effective remedy at national level.

In assessing whether the respondent State acted within its margin of appreciation while implementing bulk interception regime, Court expanded the six safeguards established in relation to targeted surveillance. Instead, it developed eight safeguards, which domestic law on bulk surveillance must contain. These are the following: 1. The grounds for authorization of bulk interception; 2. The circumstances for intercepted individual's communications; 3. The procedure for granting authorisation; 4. The procedures for selecting, examining and using intercept material; 5. The precautions when sharing the

[55] Ibid, §261.

material with other parties; 6. The limits on duration, storage and destruction of intercepted material; 7. Independent supervision of compliance with the above-mentioned safeguards and powers to address non-compliance; 8. Independent *ex post facto* review powers to address non-compliance.

The Court defined the fifth safeguard, which was not detailed examined in its previous case-law. In this regard, the Court held that transmission of data to the third parties must be accompanied by several guarantees. On the one hand, the domestic law must include legal requirements to assess necessity, proportionality and privacy interests when transferring data. On the other hand, receiving State must also have safeguards to prevent abuse.

The Court applied these general standards to circumstances of the present case.

It was a common ground between the parties that the bulk interception regime had a legal basis in domestic legislation and pursued legitimate aim of protecting national security. The central issue in the present case was whether the domestic law was accessible, foreseeable and necessary in a democratic society. For this reason, the Court examined the compliance of the contested legislation according to the following eight safeguards:

1. Grounds on which bulk interception may be authorized - The Swedish Signals Intelligence Act permitted bulk interception only for external national security threats, such as, external military threats, international terrorism, serious cross-border crime, etc. Grounds for authorization were exhaustively listed, excluding domestic criminal investigations. The Court found this safeguard satisfied;

2. The circumstances in which an individual's communications may be intercepted - Under national law, only cross-border communications might be intercepted. It excluded domestic communications. Interception conducted for technical development purposes was strictly supervised. The Court found this safeguard satisfied.

3. Procedure for granting authorization – *ex antre* authorization of every bulk interception was guaranteed by the independent Foreign Intelligence Court. An independent privacy protection representative, who protected public interests, was involved in proceedings. The Court found this safeguard satisfied.

4. Procedures for selecting, examining and using intercepted material – Under national law, domestic communications must be immediately discarded. Detailed logs of every search, selector used, time, analyst and justification were kept. And what is more, Sweden had a specific law on personal data protection. The Court found this safeguard satisfied.

5. Precautions to be taken when communicating the material to other parties – Swedish law did not require to assess the necessity, proportionality and the privacy interests before sharing intelligence with third parties. The Court considered this lack as an important shortcoming and found that this safeguard was not satisfied.

6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed – Swedish law satisfied the duration requirement as it defined maximum period for bulk interception with further possibility to renew after a full reassessment. However, national law lacked rules for non-personal data destruction, which was considered as a shortcoming.

7. Supervision was exercised by independent Foreign Intelligence Inspectorate, which was granted a broad power. It issued legally binding decisions and actively conducted inspections. The Court therefore found this safeguard satisfied.

8. Post facto review – Under Swedish law, anyone could request to investigate whether they were subject to bulk interception. The inspectorate examined the request and could cease unlawful interception or destroy obtained intelligence. However, the inspectorate had dual role. In particular, it supervised the FRA's activities and reviewed individual requests, which could lead to conflicts of interests. Although the Inspectorate was subject to audits, there was no legal obligation for audits to cover investigation of individual complaints. Moreover, complainants could not obtain reasoned decisions on their requests, granting the Inspectorate wide discretion. The Court found that this safeguard was not satisfied.

According to the above-mentioned, the Court identified three main shortcomings: the absence of a clear rule on destruction of non-personal data; the absence of a legal requirement to consider privacy interests when transmitting data; and, the absence of an

effective post facto review. The Court held that the first shortcoming had limited adverse consequences, while the second and third ones could seriously affect Article 8 rights.

In the light of the foregoing, the Court found a violation of Article 8.

This case is especially important in the mass surveillance context. It was delivered on the same day as „Big Brothers Watch and Others v. The United Kingdom". In this landmark case, the Grand Chamber explained in detail the very essence and main characteristics of mass surveillance as well as its potential risks to fundamnetal human rights, namely the right to privacy. The Court also made clear distintion between mass (bulk) and targeted surveillance. The Court also acknowledged today's reality that Contracting States actively operate mass surveillance systems and conclude intelligence sharing agreements with other states.

For the first time in its case-law, the Grand Chamber listed eigh minimum safeguards, that mass surveillance laws must satisfy. It explained in detailed manner what is considered under each safeguard and what states are required to do to comply with them. The eight minimum safeguards were applied to this case. While each safeguard was assessed seperately, the Court evaluated the system as a whole and did not attach a decisive role to any each of them. As a result, it can be conclude that while some safegurads were satisfied, certain shortcomings were significant enought to undermine the overall effectivenes of mass surveillance regimes.

2.2.2.3. Big Brother Watch and Others v. The United Kingdom (2021)[56]

Following the revelations made by Edward Snowden in 2013, three applications were lodged before the Court. The applicants claimed that their electronic communications had potentially been intercepted by UK intelligence services. They complained the Convention compliance of three surveillance regimes established by the Regulation of Investigatory Powers Act 2000 (RIPA): 1. the regime for the bulk interception of communications (Section 8(4) regime); 2. the regime for receiving intelligence from foreign intelligence services; and 3. the regime regulating the acquisition of communications data from communications service providers ("CSPs") (Chapter II regime).

[56] *Big Brother Watch and Others v. The United Kingdom* [ECHR], Nos. 58170/13 62322/14 and 24960/15, [25.05.2021].

- *Compliance of bulk interception regimes and the acquisition of communications data with Article 8 of the Convention*

The Court reiterated general principles on secret surveillance. It found that the impugned measures constituted interference with Article 8. The Court assessed justification of the interference by applying three-part test. First, the Court recognized that the interference was prescribed by law and pursued legitimate aims, among others, of protecting national security. Legal provisions regulating bulk interception system were accessible, as they were clearly defined by publicly available document.

The Court assessed the necessity of the interference in line with eight safeguards developed for mass (bulk) interception regimes. This can be summarized as follows:

1. The grounds on which bulk interception may be authorized - Under domestic law, bulk interception was permitted only when necessary to achieve legitimate purposes, including protection of national security, prevention or detection of serious crime, and safeguarding the country's economic well-being as it was relevant to national security. For national security purposes, interception was limited to activities that threatened safety or well-being of the State or aimed to undermine democratic processes. While these grounds were broadly formulated, they mainly were focused on these purposes. The Court found this safeguard satisfied.

2. The circumstances in which an individual's communications may be intercepted – national law limited bulk interception to international/external communications. These were communications sent or received outside the United Kingdom. Internal communications were not targeted but could be incidentally collected if they crossed a targeted bearer. Importantly, measures existed to minimize interception of internal communications. The Court found this safeguard satisfied.

3. The procedure to be followed for granting authorization – bulk interception was authorized by the Secretary of State, which was a part of executive and lacked independence. Moreover, strong selectors linked to identifiable persons were not subject to prior internal authorization. The warrant neither specify particular bearers, nor include an indication of the categories of selectors to be employed. In such circumstances, assessing their necessity and proportionality at the

authorization stage was impossible. The Court found that this safeguard was not satisfied.

4. The procedures to be followed for selecting, examining, and using intercept material – Under national law, analysts could access communications only after demonstrating necessity and proportionality. Access was limited in time, and subject to auditing. Also, strict rules governed copying, retention and destruction of obtained material. However, the Court identified two important deficiencies: categories of selectors were not defined at authorization stage and the Secretary of State's certificate was too broad. Despite this, the Court held that these procedures provided adequate guarantees and were sufficiently clear. The Court found this safeguard satisfied.

5. The precautions to be taken when communicating the material to other parties – National law set strict limits on disclosure of intercepted material, including the number of people who could receive it, the extent of the disclosure and the permitted number of copies. Disclosure was subject to "need-to know" principle, meaning that it could only be shared with persons, whose duties required access for an authorized purpose. Each transmission was subject to independent oversight. The Court found this safeguard satisfied.

6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased or destroyed – national law contained clear rules on the duration of interception. Warrants expired after six months for national security purposes and three months for serious crime purposes. Warrants were renewable and at the same time was subject to continuous review. If interception was no longer necessary, the Secretary of State was required to cancel a warrant. Another important guarantee was the maximum retention periods for different categories of intercept material. Once the maximum retention period was expired, materials must be automatically deleted. Also, every copy of intercept material must be destroyed as soon as its retention was no longer necessary for legitimate aims. The Court found this safeguard satisfied.

7. Supervision was carried out by independent ICC Commissioner, who was able to assess the necessity and proportionality of warrant applications, the choice of selectors, and to examine the procedures for the retention, storage and destruction. The Commissioner conducted regular inspections, after which it issued formal recommendations. Annual reports were published. The Court found this safeguard satisfied.

8. Ex post facto review was carried out by the Investigatory Powers Tribunal (the IPT). Anyone who believed that they were allegedly subjected to secret surveillance, could lodge a complaint. The IPT was empowered to examine specific allegations of unlawful interception as well as the overall Convention compliance surveillance regime. The IPT had extensive powers, including holding oral hearings, awarding compensations, canceling awards, requiring destruction of any records. It also published its legal rulings on its own website, ensuring public scrutiny. The Court found this safeguard satisfied.

According to the above-mentioned, the Court identified several main shortcomings in the United Kingdom's bulk interception regime. These were the absence of independent authorization, the failure to identify categories of selectors in warrant applications, the failure to subject selectors linked to an identifiable individual to prior internal authorization, the lack of foreseeability of the circumstances in which communications could be examined and the overly broad nature of the Secretary of State's certificate.

As for the related communications data, the Court recognized their importance in combating terrorism and serious crimes. It held that search and access to such data in respect to persons who are in the UK may be necessary and proportionality under certain circumstances. The Court reiterated that the related communications data must be protected by similar safeguards as the content of communications but the same principle is not applied to the subsequent treatment of the communications data. Under domestic law related communications data were treated in most respects similarly as content. As a result, shortcomings identified in the legal framework regulating interception of the content equally applied to communications data. At the same time, communications data benefited from many same safeguards. However, the protection of communications data was weaker in two respects. First, in contrast to the content, the use of a selector referable to a person known to be in the United Kingdom did not need additional approval. While the Court

expressed concerns about this, it did not consider this gap decisive. Second, unlike the content, related communications data were not immediately deleted and could be stored for several months. The real retention periods were not published and only disclosed during the Court proceedings, making the system not foreseeable and in breach of Article 8.

Taking into consideration identified shortcomings regarding the bulk interception regime and related communications data, the Court found that the United Kingdom's legislation violated Article 8 of the Convention.

- *Compliance of intelligence sharing regime with Article 8 of the Convention*

As a general principle, the Court held that safeguards applicable for examination, use, storage, transmission, erasure and destruction of intercepted communications as well as the requirements of independent supervision and ex post facto review apply equally when a Contracting State receives solicited intercept material from a foreign intelligence service.

The Court applied these general principles to the present case. It found that the United Kingdom's regime for requesting and receiving intelligence from foreign states had a clear legal basis in national law, in particular, intelligence sharing rules were incorporated in Chapter 12 of the Interception of Communications Code of practice, which was publicly accessible document. Therefore, intelligence sharing regime was accessible and foreseeable. Also, intelligence sharing pursued legitimate aims of protecting national security, preventing disorder and crime and protecting the rights and freedoms of others. Under national law, United Kingdom's intelligence services could request data from foreign countries only when a warrant had already been authorised, the foreign assistance was necessary, and the request was necessary and proportionate. Request without warrant was also allowed, but only in exceptional circumstances. In such cases, request must have personal approval of the Secretary of State and had to be notified to the Intelligence Commissioner.

The procedures for storing, accessing, examining, using, erasure and destroying of the intercepted material obtained from foreign states were the same as those applied to the materials obtained through UK interception. The Court already considered this procedure adequate. Independent oversight and post facto review of intelligence sharing were also ensured. In the light of the foregoing the Court found that the domestic intelligence-sharing regime was in compliance with the Convention.

Accordingly, it found no violation of Article 8 in this regard.

- *Compliance of acquisition of communications data from Communications Service Providers with Article 8 of the Convention*

In domestic proceedings, the respondent government acknowledged that access to communications data obtained from Communications Service Providers lacked sufficient guarantees. In particular, access was not limited to the investigation of serious crime and was not subject to prior authorization by independent body. Since the contested legislation did not include these protections, the Chamber held that it was not accordance with the law. The government did not challenge this finding before the Grand Chamber. The Court upheld that there had been a violation of Article 8 of the Convention.

The Grand Chamber's judgement in „Big Brothers Watch v. The United Kingdom" was its first assessment on the compatibility of the UK's mass surveillace regime with Convention since the Snowden revelations. The Court did not question the operation of mass surveillance systems as a whole if these systems meet a number of safeguards. This decisions raised serious debate among lawyers regarding the implications for state surveillance regimes. Even judges of the Gand Chamber, who participated in the examination the present application, critisized the majority decision. In particluar, judges Lemmens, Vehabović and Bošnjak in their dissenting opinion argued that the majority failed to assign proper weight to the right to private life and correspondence, which remain insufficiently protected against interference by bulk interception.[57]

[57] Ibid.

Chapter 3. Factors influencing the width of the margin of appreciation in national security surveillance cases

Analysis of surveillance cases discussed in previous chapter shows that the ECtHR clearly and explicitly gives a margin of appreciation to national authorities in choosing the means by which they can protect their national security. However, fundamental question is the breadth of the margin of appreciation, particularly, how wide or narrow it is in a given case. The scope of the margin of appreciation is not abstract and depends on the context of each case.[58] Hence, this chapter examines the factors that influence whether national authorities are granted wide or narrow margin of appreciation in national security surveillance cases. For this reason, it will first offer a general overview of the principle of proportionality and the doctrine of the margin of appreciation.

3.1. General overview of the proportionality principle and the margin of appreciation

The principle of proportionality, which was originally developed in the German legal doctrine, is of vital importance for the practical protection of human rights.[59] This principle is multidimensional. On the one hand, it requires that any interference by a state with human rights and fundamental freedom must be necessary, appropriate and reasonably justified in each case. On the other hand, the proportionality test guides a judge in balancing competing private and public interests, enabling them to weight such interests and give priority to one interest over another through fair and reasoned decision.[60]

The principle of proportionality contains several requirements. First, measures taken by public authorities must be suitable to achieve the legitimate aims pursued. This means that there must be a reasonable relationship between the means used and the legitimate goals;[61] Secondly, the measure in question must be the least restrictive and no other alternative less intrusive measure should be able to achieve the legitimate aim pursued with the same effectiveness. Third, the harm caused by restricting the right must not outweigh

[58] PARRAS, Francisco Javier Mena (2015). Democracy, diversity and the margin of appreciation: a theoretical analysis from the perspective of the international and constitutional functions of the European Court of Human Rights. *Revista Electrónica de Estudios Internacionales*. 29, 1-18 [online]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595092, 10.

[59] SWEET, Alec Stone. MATHEWS, Jud (2008). Proportionality Balancing and Global Constitutionalism. *Columbian Journal of Transnational Law*. 47, 68-149 [online]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1569344, 98-112.

[60] TRYKHLIB, Kristina (2020). The principle of proportionality in the jurisprudence of the European Court of Human Rights. *EU and comparative law issues and challenges series (ECLIC).* 4, 128-154 [online]. https://ojs.srce.hr/index.php/eclic/article/view/11899, 129.

[61] *Waite and Kennedy* [ECHR], No. 26083/94, [18-02-1999], §59. *Z and Others v. the United Kingdom* [ECHR], No. 29392/95, [10-05-2001], §93. *T.P. and K.M. v. the United Kingdom* [ECHR], No. 28945/95, [10-05-2001], §98.

the benefit gained from achieving the legitimate aims (proportionality in narrow sense).[62] The principle also requires that restrictions must not undermine the very essence of the rights concerned. As the Grand Chamber emphasized, "It must be satisfied that the limitations applied do not restrict or reduce the access left to the individual in such a way or to such an extent that the very essence of the right is impaired".[63] While assessing the Court whether a state's interference is proportionate, it applies the doctrine of the margin of appreciation.[64]

Some criticism has been expressed about the way in which the ECtHR applies proportionality principle in surveillance cases conducted for national security purposes. For example, Dr. Paul de Hert argues that although the Court has stated that secret surveillance measures are permissible under Article 8 only when they are strictly necessary for safeguarding democratic institutions, in practice the Court often examines merely whether such measures are necessary, rather strictly necessary. According to Paul de Hert, this approach results in the Court applying only a mild check of proportionality in national-security surveillance cases, rather than the stricter scrutiny which is demanded for secret surveillance.[65]

The doctrine of the margin of appreciation plays an essential role in European human rights jurisprudence. As the former president of the ECtHR, Sir Nicolas Bratz defined it, the margin of appreciation is a "valuable tool devised by the Court itself to assist it in defining the scope of its review, […] it is a variable notion which is not susceptible of precise definition"[66]. In addition to this, many legal scholars have described this doctrine as an important means to find a middle ground when cultures and legal traditions come into conflict.[67] The very essence of the doctrine is that it grants national authorities a discretion

---

[62] LURIE, Guy (2020). Proportionality and the Right to Equality. *German Law Journal*. 21, 174-196 [online]. https://www.cambridge.org/core/journals/german-law-journal/article/proportionality-and-the-right-to-equality/8D435CE149E705134E19EA19CC949B0F, 175.

[63] *Prince Hans-Adam II of Liechtenstein v. Germany* [ECHR], No. 42527/98, [12-07-2001] §44.

[64] TRYKHLIB, Kristina (2020). The principle of proportionality in the jurisprudence of the European Court of Human Rights. *EU and comparative law issues and challenges series (ECLIC).* 4, 128-154 [online]. https://ojs.srce.hr/index.php/eclic/article/view/11899, 129.

[65] LOIDEAIN, Ni Nora (2020). The approach of the European Court of Human Rights to the interception of communications. EU Data Privacy Law and Serious Crime (Oxford University Press), *Oxford Data Protection & Privacy Law Series*, 30-73 [online], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699386, 59.

[66] FRANTZIOU, Eleni (2014). The margin of appreciation doctrine in European human rights law. UCL policy briefing [online]. London: London's Global University. https://www.ucl.ac.uk/public-policy/sites/public_policy/files/migrated-files/European_human_rights_law.pdf.

[67] GERARDS, Janneke (2018). Pluralism, Margin of Appreciation and Incrementalism in the Case Law of the European Court of Human Rights. *Human Rights Law review.* 18, 495-515 [online]. https://academic.oup.com/hrlr/article/18/3/495/5068636, 498.

in applying and implementing the Convention, as the primary enforcers of its provisions.[68] It also ensures the maintenance of the supervisory role of the Court. As a result, the margin of appreciation can be considered as a "two pronged" instrument which allows the ECtHR to interpret and protect individual rights on the one hand and to respect the sovereignty of member States on the other.[69]

It should be emphasized that the term "margin of appreciation" was found neither in the text of the ECHR nor in its preparatory documents until 2021, when Protocol No. 15 entered into force and codified this doctrine explicitly into the Preamble.[70] As the explanatory report of this protocol states, the amendment was intended to enhance the transparency and accessibility of the margin of appreciation doctrine and to formally reflect this concept as it has been developed in the Court's case-law.[71]

However, before this amendment, the margin of appreciation was a judicial doctrine. It was primarily developed through the decisions of the former European Commission of Human Rights[72] and later by the Court. In particular, the first case where the ECtHR has discussed the doctrine was the landmark case of Handyside v. The United Kingdom (1976). In this case, the Court underlined that: "the machinery of protection established by the Convention is subsidiary to the national systems safeguarding human rights. The Convention leaves to each Contracting State, in the first place, the task of securing the rights and liberties it enshrines. The institutions created by it make their own contribution to this task but they become involved only through contentious proceedings and once all domestic remedies have been exhausted. By reason of their direct and continuous contact with the vital forces of their countries, State authorities are in principle in better position than the international judge to give an opinion on the exact content of these requirements as well as on the "necessity" of a "restriction" or "penalty" intended to meet them".[73] According to this definition, three main characteristics of the margin of appreciation

[68] GREER, Steven (2000). *The Margin of Appreciation: Interpretation and Discretion under the European Convention on Human Rights* [online]. Strasbourg: Council of Europe Publishing. Google Books, 5.
[69] Djik, P. van. Hoof, G.J.H. van (1998). *Theory and Practice of the European Convention on Human Rights.* Third edition [online]. Hague: Kluwer Law International. Google Books, 92.
[70] Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms (2013), No. 213. Council of Europe. *Official website of Council of Europe*, 2.
[71] Council of Europe, Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms. Explanatory Report, No. 213, Explanatory Report, https://www.echr.coe.int/documents/d/echr/Protocol_15_explanatory_report_ENG, 2.
[72] *Greece v the United Kingdom* [ECHR], No. 176/56, [26-09-1958].
[73] *Handyside v. The United Kingdom* [ECHR], No. 5493/72, [07-12-1976], §48;

doctrine can be identified: the principle of subsidiarity, diversity of Contracting States of the Convention and the "better position" rationale. Briefly explain each of them.

The principle of subsidiarity means that ensuring respect for the rights and freedoms enshrined in the Convention is primarily the task of Contracting states.[74] The ECtHR has only a supervisory role in this regard and it is not a court of fourth instance. Its task is to ensure that national authorities have remained within the limits set by the ECHR and to intervene only in cases when those authorities fail to fulfill this obligation.[75] This principle is well established in the Court's case-law and has been recently added to the preamble of the Convention.[76] The Former President of the ECtHR, Roberto Spano, emphasized the importance of this amendment as a potential starting point for the "age of subsidiarity", which would be reflected in the Court's commitment to empowering Member States to truly "bring rights home".[77] The subsidiarity principle is also reflected in the requirement to exhaust all domestic remedies, which is one of the admissibility criteria for individual applications under Article 35(1) of the ECHR.[78] The subsidiary nature of the Convention is also evident by the fact that it harmonizes the law of Contracting States around a minimum standard of protection, rather seeking absolute uniformity of national rules.[79]

Diversity of the contracting parties to the Convention is undeniable given the wide range of cultural, moral, legal, political and social traditions across Europe. Hence, achieving a unified consensus among member States in certain areas, especially in the sensitive ones, would be impossible. The margin of appreciation thus accommodates these differences.[80]

---

[74] CLAYTON, Richard. TOMLINSON, Hugh. GEORGE, Carol (2000). The law of Human Rights [online]. Oxford. Google Books, 285.
[75] European Court of Human Rights (2010). Interlaken follow up – Principle of Subsidiarity, note by the Jurisconsult [online]. https://www.echr.coe.int/documents/d/echr/2010_interlaken_follow-up_eng, 2.
[76] Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms (2013). Council of Europe. *Official website of the Council of Europe.*
[77] SPANO, Robert (2014). Universality or Diversity of Human Rights? Strasbourg in the Age of Subsidiarity. *Human Rights Law Review*. 14, 487-502 [online]. https://scispace.com/pdf/universality-or-diversity-of-human-rights-strasbourg-in-the-3vy90w8kmk.pdf, 491.
[78] European Convention on Human Rights (1950). *Official website of the Council of Europe*. Article 35 (1)
[79] BREMS, E (2001). Human Rights: Universality and Diversity [online]. The Netherlands: Kluwer Law International. Google Books, 360.
[80] KRATOCHVIL, Jan (2011). The Inflation of the Margin of Appreciation by the European Court of Human Rights, Netherlands Quarterly of Human Rights, 29(3), 324-357 [online]. https://www.corteidh.or.cr/tablas/r26992.pdf, 24.

The "better position" rationale means that national authorities are better placed than an international court to decide controversial issues as far as they have direct knowledge of their societies' needs and circumstances.[81]

Despite the fact that the margin of appreciation doctrine is well entrenched in the Court's case-law and now it is also explicitly referenced in the Preamble of the Convention, defining its precise scope is not a simple task, because it is context-dependent.[82] As the Court noted in Schalk & Kopf v Austria (2010), "the scope of the margin of appreciation will vary according to the circumstances, the subject matter and its background".[83] The width of the margin granted to national authorities depends on number of factors. For example, Paul Mahoney, a former registrar of the European Court of Human Rights identifies several factors which influence the scope of the margin of appreciation: 1. The existence of common ground among member states (European Consensus); 2. The nature of the right involved. 3. The nature of the duty incumbent on the state – whether it is a positive or a negative obligation; 4. The nature of the legitimate aim pursued by the state when interfering with the right; 5. The nature of the activity being regulated – its importance for the individual and its implications for society as a whole; 6. The circumstances of the case, and 7. The actual wording of the Convention.[84]

The following sections examine essential factors which influence the width of the margin of appreciation in national security surveillance cases.

[81] PARRAS, Francisco Javier Mena (2015). Democracy, diversity and the margin of appreciation: a theoretical analysis from the perspective of the international and constitutional functions of the European Court of Human Rights. *Revista Electrónica de Estudios Internacionales.* 29, 1-18 [online]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595092, 14.
[82] GERARDS, Janneke. FLEUREN, Joseph (2012). Implementation of the European Convention on Human Rights and of the judgments of the ECtHR in national case-law, a comparative analysis [online]. Cambridge – Antwerp – Portland. Inter-American Court of Human Rights, 29.
[83] *Schalk and Kopf v. Austria [ECHR],* No. 30141/04, [24/06/2010].
[84] MOWBRAY, J. Alastair (2007). Cases and Materials on the European Convention on Human Rights, United States. Second edition [online]. United States: Oxford University press. Google Books, 632.

3.2. Nature and seriousness of the threat to national security

The aim pursued is one of the most important factors in determining the scope of the margin of appreciation. The ECtHR has recognized a wide margin of appreciation about restriction of the right to privacy in the interest of national security.[85] Fight against terrorism actually falls within that aim. In fact, Article 8 of the Convention imposes certain positive obligations on member States to protect the general public from terrorism.[86]

The 11 September 2001 (9/11) terrorist attacks once again demonstrated that terrorism can destabilize democratic institutions and endanger the protection of human rights.[87] Hence, several scholars have argued that terrorism justifies a wider margin of appreciation. In particular, Yourow believes that anti-terrorism interest requires a wide margin because they are highly sensitive isssues, which concern the protection of large numbers of people. [88]The same approach is shared by Aria-Takahashi who links national security to state sovereignity and considers that this interest is a prone to a wide margin.[89] Warbrick also notes that the „background of terrorism" can lead to a broader margin.[90] After analyzing the relevant judgements delivered by the ECtHR, B. Latos concludes that State authorities must apply a number of measures to combat espionage and foreign intelligence as they pose a threat to the stability of the State.[91]

The ECtHR also makes it clear that „in assessing the pressing social need [...] and in particular in choosing the means for achieving the legitimate aim of protecting national security, [is] a wide one."[92] Accordingly, the Court is willing to grant state authoroties a wide margin to combat terrorism as far as it acknowledges that states have a legitimate need to combat terrorism as well as terrorists.[93] However, the fact that a case concerns terrorism

---

[85] Open Society Justice Initiative (2012), *Margin of Appreciation: An overview of the Strasbourg Court's margin of appreciation doctrine* [online]. https://www.justiceinitiative.org/uploads/918a3997-3d40-4936-884b-bf8562b9512b/echr-reform-margin-of-appreciation.pdf, 2.

[86] Council of Europe (2025), Guide on case-law of the European Court of Human Rights– Terrorism, https://ks.echr.coe.int/documents/d/echr-ks/guide_terrorism_eng, 9.

[87] European Commission for Democracy Through Law (Venice Commission) (15-12-2015). Report on the democratic oversight of signals intelligence agencies [online]. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e, 8.

[88] YOUROW, Howard Charles (1996). The margin of appreciation doctrine in the dynamics of European Human Rights Jurisprudence [online], the Netherlands: Martinus Nijhoff Publishers. Google Books, 21.

[89] ARAY, Yutaka (2001). The margin of appreciation doctrine and the Principe of proportionality in the jurisprudence of the ECHR [online], Oxford: Intersentia 2001. Google Books, 209.

[90] WARBRICK, Colin (2004). The European Response to Terrorism in an Age of Human Rights. T*he European Journal of International Law,* 15, 989-1018, [online] https://academic.oup.com/ejil/article/15/5/989/533500, 1002.

[91] FERENC-KOPEC, Dorota (2017). National security as a legitimate excuse to human rights restrictions. *Human rights: between needs and possibilities,* 91-103, [online]. https://www.wydawnictwo.wsge.edu.pl/pdf-138085-64909?filename=64909.pdf, 99.

[92] *Leander v. Sweden* [ECHR], No. 9248/81, [26-03-1987], §59.

[93] *Gillan and Quinton v. the United Kingdom* [ECHR], No. 4158/05, [12-01-2010].

or a particular measure aims to prevent terrorist activity does not exempt it from European supervision. The ECtHR has not developed a special approach for terrorism-related cases and they are examined within the same general framework, which apply to other Article 8 cases.[94] This means that High Contracting Parties are not allowed to act in any manner they deem appropriate to combat terrorism.

This is clearly illustrated in "SZABÓ and VISSY v. Hungary", where secret surveillance aimed to the prevention, tracking and repelling of terrorists acts in the respondent state.[95] While this aim was considered legitimate under Article 8(2), the Court found a violation of Article 8 of the Convention, because of the insufficient guarantees in domestic law and unfiltered power granted to national authorities. Similarly, in "Klass and Others v. Germany", the Court reiterated that democratic societies face increasingly sophisticated forms of espionage and terrorism. Therefore, the domestic authorities were granted a discretion in setting the conditions for secret surveillance to fight against terrorism, because it was necessary in a democratic society in the interests of national security and prevention of crime. However, the Court emphasized that states do not have unlimited discretion to subject persons to secret surveillance measures in the name of the struggle against espionage and terrorism.[96] In that case, however, the German law provided adequate guarantees against abuse and the Court found no violation of Article 8.

The same approach was taken in the landmark case of "Kennedy v. the United Kingdom", where interception measures aimed to protect national security in the context of citizens terrorist and organized crimes threats. However, the Court found no violation of Article 8, because the domestic law on interception clearly defined the authorization procedures, processing of intercepted materials, as well as the processing, communicating and destruction of intercept material collected.[97]

To sum up, States are granted a wide margin of appreciation in evaluating threats to national security and choosing appropriate means to address it, including by operating secret surveillance. Therefore, terrorism, cyber-attacks, espionage and other serious organized crimes influence on the breadth of the margin of appreciation. However, this broader margin is granted only where the domestic legislation contains sufficient, clear and

[94] ALAMER, Fahad (2022). The Regime of European Court of Human Rights in Migration and Terrorism, *Kilaw Journal*, 10, 38-68 [online]. https://journal.kilaw.edu.kw/wp-content/uploads/2022/08/37-68-A.-Fahad-Al-Amer.pdf, 50.
[95] *Szabó and Vissy v. Hungary* [ECHR], no. 37138/14, [12.01.2016], §55.
[96] *Klass and Others v. Germany* [ECHR], No. 5029/71, [06.09.1978], §§48-49.
[97] *Kennedy v. the United Kingdom* [ECHR], No. 26839/05, [18-05-2010], §169.

effective safeguards against abuse. Without such guarantees, states cannot rely on only terrorism or other national security threats to justify surveillance powers.

3.3. Quality of domestic law and guarantees

The ECtHR has remarked that even when national security is at stake, the concepts of lawfulness and the rule of law must be respected.[98] Particularly, in case "Janowiec and Others v. Russia" (2013), the Grand Chamber emphasized that "even where national security is at stake, the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and the relevant evidence. If there was no possibility of challenging effectively the executive's assertion that national security was at stake, the State authorities would be able to encroach arbitrarily on rights protected by the Convention".[99]

Indeed, case-law of the ECtHR clearly demonstrates that the requirement that an interference must be "in accordance with law" has become one the key testing standards in secret surveillance cases for assessing the lawfulness and proportionality of the state's interferences within the right to privacy in the name of protecting national security.[100] It should be noted that the requirement of lawfulness is one of the main reflections of the Rule of Law, which is explicitly enshrined in Article 3 of the Statute of the Council of Europe[101] and in the Preamble to the Convention.[102] The former president of the ECtHR, Linos-Alexandre Sicilianos, in his speech delivered in Montenegro in 2020 during a round table on the Rule of Law and the European Court of Human Rights, emphasized the importance of this principle in a democratic society.[103]

---

[98] KOPEC, Ferenc (2017). National security as a legitimate excuse to human rights restrictions. *Human rights: between needs and possibilities*, 91-103 [online]. https://www.wydawnictwo.wsge.edu.pl/pdf-138085-64909?filename=64909.pdf, 97.

[99] *Janowiec and Others v. Russia* [ECHR]. Nos. 55508/07 and 29520/09, [21-10-2013], §213.

[100] BIGO, Didier. CARRERA, Sergio. HERNANZ, Nicholas. JEANDESBOZ, Julien. PARKIN, Joanna. RAGAZZI, Francesco. SCHERRER, Amandine (2013). Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law. *CEPS Paper in Liberty and Security in Europe,* 61, 1-60 [online]. https://cdn.ceps.eu/wpcontent/uploads/2013/11/No%2062%20Surveillance%20of%20Personal%20Data%20by%20EU%20MSs.pdf, 21.

[101] Statute of the Council of Europe (1949). Council of Europe. *Official website of the Council of Europe*. Article 3.

[102] European Convention on Human Rights (1945). Council of Europe. *Official website of the Council of Europe*. Preamble.

[103] European Court of Human Rights (2020). The Rule of Law and the European Court of Human Rights: the independence of the judiciary, Montenegrin Academy of Sciences and Arts, Montenegro, [online], https://www.echr.coe.int/documents/d/echr/Speech_20200228_Sicilianos_Montenegro_ENG, 2-3.

While the concept of the Rule of Law has not been defined explicitly in any binding legal text, not by the ECtHR, its core elements still can be identified.[104] For example, the Venice Commission notes that universally recognized elements of the Rule of Law include legality, legal certainty, foreseeability, prevention of abuse of powers, equality before the law, non-discrimination and access to justice. The aim of these elements, taken together, is to protect the individuals from arbitrariness, especially when they are in relation to the State.[105]

The principle of the Rule of Law first appeared in the ECtHR's case-law in Golder v. United Kingdom (1975). In this judgement, the Court stated that the Rule of Law was one of the main reasons why the signatory states decided to guarantee and enforce fundamental human rights and freedoms guaranteed by the Universal Declaration of Human Rights.[106] Since this case, the Rule of Law principle has become a guiding principle of the Court's jurisdiction.[107]

In cases where secret surveillance measures are applied on national security grounds, the requirement of lawfulness means that national law must provide clear and detailed rules governing the surveillance system. It must be accessible and formulated with sufficient precision to enable the person concerned to foresee its consequences. The circumstances and the conditions under which public authorities are empowered to resort to such measures must also be set out in law. The law must also indicate the scope of any discretion of the competent authorities and the manner of its exercise with sufficient clarity to give individuals adequate protection against arbitrary interference.[108] The purpose of defining powers with precision is to reduce the scope for misuse or excess power.[109]

---

[104] European Court of Human Rights (2025). 75 years of the European Convention on Human rights Focus On: The Rule of Law [online], https://ks.echr.coe.int/documents/d/echr-ks/focus-on-the-rule-of-law, 1.
[105] European Commission for Democracy Through Law (Venice Commission) (11-12-2016). 106th plenary session [online]. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-PL-PV(2016)001-bil, §16.
[106] *Golder v. United Kingdom* [ECHR]. No. 4451/70, [21-02-1975], §34.
[107] *Engel and Others v. the Netherlands* [ECHR]. Nos. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, [08-06-1976], § 69. *Winterwerp v. the Netherlands* [ECHR]. No. 6301/73, [24-10-1979], § 39.
[108] Council of Bars & Law Societies of Europe (2019). CCBE recommendations on the protection of fundamental rights in the context of "national security" [online], https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf, 7-8.
[109] European Commission for Democracy Through Law (Venice Commission) (15-12-2015). Report on the democratic oversight of signals intelligence agencies [online]. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-, 23.

In this regard, it is important to refer to the study prepared for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, entitled "Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law". In this study landmark cases are compared to demonstrate the decisive role played by the quality of domestic law and the existence of guarantees in determining the extent of the margin of appreciation. The authors of this study analyze several landmark cases of the ECtHR. First, they note the Weber and Saravia case – already discussed in this thesis – which shows that the main reason why the application was declared dismissed was the high quality of German legislation governing secret surveillance and the incorporated safeguards against abuse. These guarantees convinced the Court that such measures were necessary to protect the respondent State's (Germany's) national security.

On the other hand, in Liberty and Others v. the United Kingdom, the contested legislation lacked a sufficiently predictable legal basis satisfying the accessibility principle and failed to provide adequate protection against abuse. In case Kennedy v. the United Kingdom the Court once again stressed that the domestic law on which interference is prescribed must be compatible with the rule of law and accompanied by sufficient guarantees. This comparison reflects the standard established by the ECtHR according to which, granting discretion to the national authorities in terms of an unfettered power is contrary to the rule of law.[110]

According to the above-mentioned, the Court grants a wide margin of appreciation to national authorities to uphold national security only when adequate and sufficient guarantees are in place.[111] It is apparent from the ECtHR's case-law that the two most significant safeguards in surveillance-related cases where national security is at stake, are the independent authorization process and the follow-up oversight process. This approach is shared by the professor Douwe Korff[112] and by the scholar Nóra Ní Loideain who

[110] BIGO, Didier. CARRERA, Sergio. HERNANZ, Nicholas. JEANDESBOZ, Julien. PARKIN, Joanna. RAGAZZI, Francesco. SCHERRER, Amandine (2013). Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law. *CEPS Paper in Liberty and Security in Europe,* 61, 1-60 [online]. https://cdn.ceps.eu/wpcontent/uploads/2013/11/No%2062%20Surveillance%20of%20Personal%20Data%20by%20EU%20MSs.pdf, 21-23.

[111] NUGRAHA, Ignatius Yordan. REGULES, Juncal Montero. VRANCKEN, Merel (2022). Big Brother Watch and Others v. the United Kingdom, *The American Journal of International Law,* 585-592 [online], https://www.cambridge.org/core/services/aop-cambridge core/content/view/024BF9DDDFA0C882358B052845230352/S0002930022000355a.pdf/big-brother-watch-and-others-v-the-united-kingdom.pdf, 588.

[112] KORFF, Douwe (2013). Note on European & International Law on trans-national surveillance prepared for the civil liberties committee of the European Parliament to assist the Committee in its enquires into USA and European States' surveillance. https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf, 4.

mentions that in assessing the proportionality of both bulk and targeted interception regimes much consideration is given to supervisory controls governing the authorization and oversight as they show that the relevant authorities are properly applying the law in practice and prevent deliberate abuse of power.[113] Independence of authorizing and oversight body is a decisive factor. As the ECtHR held in "IORDACHI and Others v. Moldova" (2009) and "EKIMDZIEV v. Bulgaria (2022), independent controls must exist on authorization and oversight stages.[114] As mentioned previously, independent oversight mechanism has become even more important in relation to bulk surveillance in the context of "end-to-end" safeguards. But it does not mean that the existence of independent authorizing and/or oversight mechanisms automatically constitutes convention compliance to the legislation governing surveillance regimes.

To sum up, the requirement of lawfulness and respect for the rule of law is a decisive factor in determining the scope of the margin on appreciation in national security surveillance cases. The better the quality of the domestic law and the stronger the guarantees against abuse, the wider the margin of appreciation afforded to national authorities - meaning that the Court is more likely to find that they have not overstepped their margin.

3.4. European Consensus and the rights and interests involved

The European Consensus standard refers to the existence or non-existence of a common ground in the laws and practices of the Member States. It reflects the idea that the Convention is a living instrument, which must be interpreted in the light of present-day conditions and the Court must consider the changing conditions in contracting states and respond to any emerging consensus as to the standards to be achieved.[115] Analysis of the case-law makes it clear that where a European consensus exists on a particular issue, national authorities are generally granted a narrower margin of appreciation. In contrast to this, when there is no consensus on morally, legally, cultural and/or religiously sensitive issues among European States, they enjoy a wider margin of appreciation.[116] This measns that when the Contracting States have no consensus on the relative importance of the

[113] LOIDEAIN, Ni Nora (2020). The approach of the European Court of Human Rights to the interception of communications. EU Data Privacy Law and Serious Crime (Oxford University Press), *Oxford Data Protection & Privacy Law Series*, 30-73 [online], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699386, 66.
[114] *IORDACHI and Others v. Moldova* [ECHR], No. 25198/02, [10-02-2009], §40. *EKIMDZIEV v. Bulgaria* [ECHR], No. 70078/12, [11-01-2022], §294.
[115] *Chapman v. The United Kingdom* [ECHR], No. 27238/95, [18- 01-2001]. *Tyrer v. The United Kingdom* [ECHR], No. 5856/72, [25-04-1978], §31.
[116] *A, B and C v. Ireland* [ECHR], No. 25579/05, [16-12-2010], §5.

interest at stake, or as on the means of protecting it, the margin of appreciation will be broader.[117]

In secret surveillance cases, the ECtHR has tended to grant States a wider margin in matters of national security, given the sensitive and confidential nature of the information involved and the seriousness of the threat at the material time. Case-law illustrate that factors such as the threats posed by the "scourge of global terrorism" and "the increased sophistication of communications technology" have influenced the Court's assessment in favor of a wider margin.[118]

The nature of the right involved and the interest at stake are also important factors in determining the scope of the margin of appreciation. For example, the ECtHR recognized a wide margin of appreciation about restriction of the right to privacy in the interest of national security. However, the margin will tend to be narrower where the right concerned is crucial to the individual's private life or key for the effective enjoyment of intimate or fundamental aspects of their identity.[119] In particular, where a measure affects a particularly important aspects of a person's important facet existence or identity, the margin of appreciation becomes more restricted.[120]

In parallel to the above-mentioned factors, it cannot be overlooked that the type of secret surveillance measures also effects the breadth of the margin of appreciation. As the case-law of the ECtHR clarifies, national authorities are granted a wider margin of appreciation when applying targeted surveillance. On the other hand, given the indiscriminate nature of mass (bulk) surveillance, the Court examines the margin afforded to state authorities with greater scrutiny. It is reflected by the fact that the ECtHR does not consider the Weber safeguards sufficient for mass (bulk) surveillance and expands them.

To conclude, the existence or absence of European Consensus as well as the right involved, the aim pursued and the type of surveillance measures all effect the breadth of the margin of appreciation. However, these factors are assessed together and none of them has decisive importance by itself.

---

[117] *Dickson v. the United Kingdom* [ECHR], No. 44362/04, [44362/04], § 78.
[118] LOIDEAIN, Ni Nora (2020). The approach of the European Court of Human Rights to the interception of communications. EU Data Privacy Law and Serious Crime (Oxford University Press), *Oxford Data Protection & Privacy Law Series*, 30-73 [online], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699386, 63.
[119] *Connors v. the United Kingdom* [ECHR], No. 66746/01, [27-05-20004], § 82.
[120] *Evans v. the United Kingdom* [ECHR], No. 6339/05, [10-04-2007], § 77.

CONCLUSIONS

The analysis of the case-law of the ECtHR and the relevant materials clearly demonstrates that national security constitutes one of the most frequently invoked legitimate aims to justify an interference with the right to privacy under Article 8 of the ECHR, especially in the context of secret surveillance regimes.

While the notion "national security" is not precisely defined by the ECtHR, its case-law shows that this concept is closely linked to the protection of State sovereignty and democratic institutions from serious threats such as terrorism, espionage, cyberattacks and other forms of serious organized crimes. Secret surveillance is considered as one of the most effective and essential means for addressing such threats and therefore is not prohibited by the Convention, including in the form of bulk interception, which is not *per se* incompatible with the Article 8 of the ECHR. Instead, the Court assesses the proportionality of each interference by applying its well-established three-part test, which in surveillance-related cases has specific meaning, particularly regarding the foreseeability requirement and the admissibility of individual applications lodged *in abstracto*.

An important finding is that the margin of appreciation plays an essential role in determining how high contracting states of the Convention assess threats to national security and choose appropriate means to responded them, including by means of secret surveillance. However, there is no consistent theory by the Court on the use of the margin of appreciation and discussing on its breadth is possible on the basis of its case-law. The analysis shows that several key factors influencing the scope of the margin of appreciation secret surveillance-related cases include the seriousness of the threat, existence or absence of European consensus, the aim pursued, the right involved, the quality of domestic law and the presence of adequate and sufficient guarantees against abuse and arbitrariness.

It is welcomed that the ECtHR attaches a significant importance to the requirement of lawfulness, the rule of law principle and the need for national safeguards and guarantees against abuse. This is reflected in the fact that the ECtHR has developed well-established the minimum safeguards for targeted and mass (bulk) surveillance. However, several shortcomings can be identified in this regard.

In particular, the case-law of the ECtHR on both targeted and mass (bulk) surveillance makes it clear that although the Court assesses each safeguard separately and indicates whether each of them is satisfied, its final conclusion on whether there has been a violation

of the right to privacy under Article 8 does not depend on the absence of one or more specific safeguards. Instead, it assesses the sufficiency and effectiveness of the safeguards as a whole. The analysis of the relevant case-law (discussed above) supports this finding, because in some cases domestic legislation lacked one or more minimum safeguards, but other guarantees counterbalanced them and the Court found no violation. On the other hand, in some cases the absence of one or more minimum safeguards led the ECtHR to find a violation of Aticle8 of the ECHR.

The ECtHR explicitly mentions that it conducts a global assessment in secret surveillance cases involving national security. While a global assessment is not per se problematic, it raises several concerns. First, it should be reiterated that these cases concern to interferences with private life and correspondence in the context of surveillance in the name of national security. Both the right to privacy and the protection of national security have essential importance in a democratic society and every judgement of the ECtHR plays a crucial role in striking a fair balance between them.

The case-law of the ECtHR clarifies that none of the minimum safeguards is a self-standing requirement and that non-compliance with one or more such safeguards may be repaired by applying a global assessment. This is problematic for several reasons. First, the ECtHR does not specify which safeguard(s) can counterbalance the absence which others. Such approach may be confusing for national authorities and led to arbitrariness. Notably, a High Contracting party of the Convention may observe that the Court has accepted surveillance regimes lacking retain safeguards and therefore assume that including only some of them in domestic legislation, will be justified as a whole through the global assessment.

Furthermore, minimum safeguards are considered as absolute limits, which require a stricter and more foreseeable protection especially in the field of secret surveillance, which is not transparent to the public. However, the case law does not clarify the relative weight of each safeguard. At the same time, in other areas of alleged violation of human rights, the absence of a single procedural guarantees can be decisive. For example, in cases concerning the testimony of an absent witness, the absence of a good reason for nonappearance have found as a decisive factor for finding a violation of the right to a fair trial under Article 6 of the Convention.

To sum up, the ECtHR should be more precise about the minimum safeguards, and should provide a clearer guidance on their substantive content, what is required under each of them, and the weight each of them. If the absence of one or more safeguards does not automatically lead to a violation of article 8, the Court should explain then which safeguards can be balanced for the absence of others and under what circumstances.

According to the above-mentioned findings, several recommendations can be made. First, in surveillance-related cases concerning the protection of national security as a legitimate ground for the restricting the right to privacy, the ECtHR uses varying terminology regarding the breadth of the margin of appreciation. In particular, in different cases (discussed above), the Court refers to "a certain margin of appreciation", "a fairly wide margin of appreciation", and "a certain discretion". Such inconsistency in terminology may cause confusion, because the notion of "a certain discretion" or "a certain margin of appreciation" do not clearly indicate whether this margin is narrow or wide. Therefore, the use of a unified terminology in cases concerning the interrelation of surveillance regimes, national security and the right to privacy would be helpful explicitly identify whether state authorities are granted a wide or narrow margin of appreciation. What is more, the ECtHR should be more precise about the content and weight of the minimum safeguards well-established in its case-law to avoid any arbitrary or abusive interpretation of them.

LIST OF SOURCES

1. Legal acts

1.1. Charter of Fundamental Rights of the European Union (2000). European Union. *Official Journal of the European Communities*, 2000, C 364/1.

1.2. Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms (2013), No. 213. Council of Europe. *Official website of Council of Europe*.

1.3. European Convention on Human Rights (1950). *Official website of Council of Europe*.

1.4. International Covenant on Civil and Political Rights (1966). United Nations. *Official website of the United Nations*.

1.5. Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms (2013). Council of Europe. *Official website of Council of Europe.*

1.6. Statute of the Council of Europe (1949). Council of Europe. *Official website of the Council of Europe*.

1.7. Universal Declaration of Human Rights (1948). United Nations. *Official website of the United Nations.*

1.8. Regulation No 2024/1689 of the European Parliament and of the Council of 13 June 2023 on laying down harmonized rule son artificial intelligence and amending regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). OJ L, 12.7.2024.

2. Case law

2.1. **Decisions of the European Court of Human Rights (ECtHR)**

2.1.1. *A, B and C v. Ireland* [ECHR], No. 25579/05, [16-12-2010].

2.1.2. *Bédat v. Switzerland [*ECHR], No. 56925/08, [29-03-2016].

2.1.3. *Big Brother Watch and Others v. The United Kingdom* [ECHR], Nos. 58170/13 62322/14 and 24960/15, [25.05.2021].

2.1.4. *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [ECHR], No. 45036/98, [30-06-2005].

2.1.5. Centrum för rättvisa v. Sweden [ECHR], No. 25252/08, [25-05-2021].

2.1.6. *C.G. and Others v. Bulgaria* [ECHR], No. 1365/07, [24-04-2008].

2.1.7. *Connors v. the United Kingdom* [ECHR], No. 66746/01, [27-05-20004].

2.1.8. *Dickson v. the United Kingdom* [ECHR], No. 44362/04, [44362/04].

2.1.9. *Drelon v. France* [ECHR], Nos. 3153/16 and 27758/18, [08-09-2022].

2.1.10. *Engel and Others v. the Netherlands* [ECHR]. Nos. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, [08-06-1976].

2.1.11. *Evans v. the United Kingdom* [ECHR], No. 6339/05, [10-04-2007].

2.1.12. *Esbester v. the United Kingdom* [ECHR], No. 18601/91, [02-04-1993].

2.1.13. *Golder v. United Kingdom* [ECHR]. No. 4451/70, [21-02-1975].

2.1.14. *EGELAND and HANSEID v. Norway* [ECHR], No. 34438/04, [16-04-2009].

2.1.15. *EKIMDZIEV v. Bulgaria* [ECHR], No. 70078/12, [11-01-2022].

2.1.16. *Chapman v. The United Kingdom* [ECHR], No. 27238/95, [18- 01-2001].

2.1.17. *Greece v the United Kingdom* [ECHR], No. 176/56, [26-09-1958].

2.1.18. *Giacomeli v. Italy* [ECHR], No. 59909/00, [02-11-2006].

2.1.19. *Gillan and Quinton v. the United Kingdom* [ECHR], No. 4158/05, [12-01-2010].

2.1.20. *Halford v. The United Kingdom* [ECHR], No. 20605/92, [25-06-1997].

2.1.21. *Handyside v. The United Kingdom* [ECHR], No. 5493/72, [07-12-1976].

2.1.22. *Hewitt and Harman v. the United Kingdom* [ECHR], No. 20317/92, [01-09-1993].

2.1.23. *Huvig v. France* [ECHR], No. 11105/84, [24-04-1990].

2.1.24. *IORDACHI and Others v. Moldova* [ECHR], No. 25198/02, [10-02-2009].

2.1.25. *Janowiec and Others v. Russia* [ECHR]. Nos. 55508/07 and 29520/09, [21-10-2013].

2.1.26. *Kennedy v. the United Kingdom* [ECHR], No. 26839/05, [18-05-2010].

2.1.27. *Klass and Others v. Germany* [ECHR], No. 5029/71, [06.09.1978].

2.1.28. *Kroon and Others v. the Netherlands* [ECHR], No. 18535/91, [27-10-1994].

2.1.29. *Leander v. Sweden* [ECHR], No. 9248/81, [26-03-1987].

2.1.30. *Liberty and Others v. the United Kingdom* [ECHR], No. 58243/00, [01-07-2008].

2.1.31. *Malone v. the United Kingdom* [ECHR], No. 8691/79, [02-08-1984].

2.1.32. *N.D. and N.T. v. Spain* [ECHR], Nos. 8675/15 and 8697/15, [13-02-2020].

2.1.33. *Niemietz v. Germany* [ECHR], No. 13710/88, [16-12-1992].

2.1.34. *Prince Hans-Adam II of Liechtenstein v. Germany* [ECHR], No. 42527/98, [12-07-2001].

2.1.35. *Roman Zakharov v. Russia* [ECHR], No. 47143/06, [04-12-2015].

2.1.36. *Rotaru v. Romania* [ECHR], No. 28341/95, [04-05-2000].

2.1.37. *S. and Marper v. the United Kingdom* [ECHR], Nos. 30562/04 and 30566/04, [04-12-2008].

2.1.38. *Schalk and Kopf v. Austria [ECHR],* No. 30141/04, [24/06/2010].

2.1.39. *Szabó and Vissy v. Hungary* [ECHR], no. 37138/14, [12.01.2016].

2.1.40. *T.P. and K.M. v. the United Kingdom* [ECHR], No. 28945/95, [10-05-2001].

2.1.41. *Tyrer v. The United Kingdom* [ECHR], No. 5856/72, [25-04-1978].

2.1.42. *Waite and Kennedy* [ECHR], No. 26083/94, [18-02-1999].

2.1.43. *Weber and Saravia v. Germany* [ECHR], No. 54934/00, [29.06.2006].

2.1.44. *Winterwerp v. the Netherlands* [ECHR]. No. 6301/73, [24-10-1979.

2.1.45. *Z and Others v. the United Kingdom* [ECHR], No. 29392/95, [10-05-2001].

2.1.46. *Z v Finland* [ECHR], No. 22009/93, [25-02-1997].

2.2.**Decisions of the Court of Justice of the European Union (CJEU)**

2.2.2. *La Quadrature du Net and Others*, [CJEU], Nos. C-511/18, C-512/18 and C-520/18, [06.10.2020].

2.2.3. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters [GCHQ], Security Service [MI5], Secret Intelligence Service [MI6]* [CJEU], No. C-623/17, [15.10.2020].

2.3. **Decisions of the U.S. Supreme Court**

2.3.1. The U.S. Supreme Court. Decision of 4 June 1928 in a criminal case Nos. 493, 532 and 533.

3. Literature

3.1.Books

3.1.1. ARAY, Yutaka (2001). The margin of appreciation doctrine and the Principe of proportionality in the jurisprudence of the ECHR [online], Oxford: Intersentia 2001. Google Books.

3.1.2. BREMS, E (2001). Human Rights: Universality and Diversity [online]. The Netherlands: Kluwer Law International. Google Books.

3.1.3. CLAYTON, Richard. TOMLINSON, Hugh. GEORGE, Carol (2000). The law of Human Rights [online]. Oxford. Google Books.

3.1.4. COOLEY, Thomas M (1888). A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract. Second edition [online]. Chicago: Callaghan & Company. Google Books.

3.1.5. Djik, P. van. Hoof, G.J.H. van (1998). Theory and Practice of the European Convention on Human Rights. Third edition [online]. Hague: Kluwer Law International. Google Books.

3.1.6. GERARDS, Janneke. FLEUREN, Joseph (2012). Implementation of the European Convention on Human Rights and of the judgments of the ECtHR in national case-law, a comparative analysis [online]. Cambridge – Antwerp – Portland. Inter-American Court of Human Rights.

3.1.7. GREER, Steven (2000). The Margin of Appreciation: Interpretation and Discretion under the European Convention on Human Rights [online]. Strasbourg: Council of Europe Publishing. Google Books.

3.1.8. HARRIS, David John; O'BOYLE, Michael; BATES, Ed and etc. (2023). *Law of the European Convention on Human Rights*. Fifth edition [online]. Oxford: Oxford University Press. Google Books.

3.1.9. MOWBRAY, J. Alastair (2007). Cases and Materials on the European Convention on Human Rights, United States. Second edition [online]. United States: Oxford University press. Google Books.

3.1.10. NISSENBAUM, Helen (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life [online]. Standford, California: Stanford University Press. Google Books.

3.1.11. YOUROW, Howard Charles (1996). The margin of appreciation doctrine in the dynamics of European Human Rights Jurisprudence [online], the Netherlands: Martinus Nijhoff Publishers. Google Books.

3.2. Articles

3.2.1. BIGO, Didier. CARRERA, Sergio. HERNANZ, Nicholas. JEANDESBOZ, Julien. PARKIN, Joanna. RAGAZZI, Francesco. SCHERRER, Amandine (2013). Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law. *CEPS Paper in Liberty and Security in Europe,* 61, 1-60 [online]. https://cdn.ceps.eu/wpcontent/uploads/2013/11/No%2062%20Surveillance%20of%20Personal%20Data%20by%20EU%20MSs.pdf.

3.2.2. ÇALI, Başak (2018). Balancing Test: European Court of Human Rights (ECtHR). *Oxford Public International Law* [online].

https://opil.ouplaw.com/display/10.1093/law-mpeipro/e3426.013.3426/law-mpeipro-e3426.

3.2.3. GAVISON, Ruth (1980). Privacy and the Limits of Law. *The Yale Law Journal*. 89, 421-471 [online]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957.

3.2.4. FERENC-KOPEC, Dorota (2017). National security as a legitimate excuse to human rights restrictions. *Human rights: between needs and possibilities,* 91-103, [online]. https://www.wydawnictwo.wsge.edu.pl/pdf-138085-64909?filename=64909.pdf.

3.2.5. FRANTZIOU, Eleni (2014). The margin of appreciation doctrine in European human rights law. UCL policy briefing [online]. London: London's Global University. https://www.ucl.ac.uk/public-policy/sites/public_policy/files/migrated-files/European_human_rights_law.pdf.

3.2.6. GERARDS, Janneke (2018). Pluralism, Margin of Appreciation and Incrementalism in the Case Law of the European Court of Human Rights. *Human Rights Law review.* 18, 495-515 [online]. https://academic.oup.com/hrlr/article/18/3/495/5068636.

3.2.7. KOPEC, Ferenc (2017). National security as a legitimate excuse to human rights restrictions. *Human rights: between needs and possibilities*, 91-103 [online]. https://www.wydawnictwo.wsge.edu.pl/pdf-138085-64909?filename=64909.pdf.

3.2.8. KRATOCHVIL, Jan (2011). The Inflation of the Margin of Appreciation by the European Court of Human Rights, *Netherlands Quarterly of Human Rights,* 29(3), 324-357 [online]. https://www.corteidh.or.cr/tablas/r26992.pdf.

3.2.9. LOIDEAIN, Ni Nora (2020). The approach of the European Court of Human Rights to the interception of communications. EU Data Privacy Law and Serious Crime (Oxford University Press), *Oxford Data Protection & Privacy Law Series*, 30-73 [online], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699386.

3.2.10. LURIE, Guy (2020). Proportionality and the Right to Equality. *German Law Journal*. 21, 174-196 [online]. https://www.cambridge.org/core/journals/german-law-journal/article/proportionality-and-the-right-to-equality/8D435CE149E705134E19EA19CC949B0F.

3.2.11. MURRAY, John L (2011). The Influence of the European Convention on Fundamental Rights on Community Law. *Fordham International Law Journal,* 33, 1388-1422 [Online]. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2208&context=ilj&httpsredir=1&referer=.

3.2.12. NUGRAHA, Ignatius Yordan. REGULES, Juncal Montero. VRANCKEN, Merel (2022). Big Brother Watch and Others v. the United Kingdom, *The American Journal of International Law,* 585-592 [online], https://www.cambridge.org/core/services/aop-cambridge-core/content/view/024BF9DDDFA0C882358B052845230352/S0002930022000355a.pdf/big-brother-watch-and-others-v-the-united-kingdom.pdf.

3.2.13. PARRAS, Francisco Javier Mena (2015). Democracy, diversity and the margin of appreciation: a theoretical analysis from the perspective of the international and constitutional functions of the European Court of Human Rights. *Revista Electrónica de Estudios Internacionales*. 29, 1-18 [online]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595092.

3.2.14. SPANO, Robert (2014). Universality or Diversity of Human Rights? Strasbourg in the Age of Subsidiarity. *Human Rights Law Review.* 14, 487-502 [online]. https://scispace.com/pdf/universality-or-diversity-of-human-rights-strasbourg-in-the-3vy90w8kmk.pdf.

3.2.15. SWEET, Alec Stone. MATHEWS, Jud (2008). Proportionality Balancing and Global Constitutionalism. *Columbian Journal of Transnational Law*. 47, 68-149 [online]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1569344.

3.2.16. TRIPKOVIC, Bosko (2022). A New Philosophy for the Margin of Appreciation and European Consensus. *Oxford Journal of Legal Studies.* 42, 207-234 [online]. https://academic.oup.com/ojls/article/42/1/207/6377894.

3.2.17. TRYKHLIB, Kristina (2020). The principle of proportionality in the jurisprudence of the European Court of Human Rights. *EU and comparative law issues and challenges series (ECLIC).* 4, 128-154 [online]. https://ojs.srce.hr/index.php/eclic/article/view/11899.

3.2.18. WARBRICK, Colin (2004). The European Response to Terrorism in an Age of Human Rights. T*he European Journal of International Law,* 15, 989-1018, [online] https://academic.oup.com/ejil/article/15/5/989/533500.

4. Internet Sources

4.1. Council of Bars & Law Societies of Europe (2019). CCBE recommendations on the protection of fundamental rights in the context of "national security" [online], https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-

Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf.

4.2. Council of Europe (2013). *National security and European case-law* [online]. https://rm.coe.int/168067d214.

4.3. Council of Europe (2018). *Mass Surveillance* [online]. https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e.

4.4. Council of Europe (2025), Guide on case-law of the European Court of Human Rights– Terrorism, https://ks.echr.coe.int/documents/d/echr-ks/guide_terrorism_eng.

4.5. Council of Europe, Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms. Explanatory Report, No. 213, Explanatory Report, https://www.echr.coe.int/documents/d/echr/Protocol_15_explanatory_report_ENG.

4.6. European Commission for Democracy Through Law (Venice Commission) (15-12-2015). Report on the democratic oversight of signals intelligence agencies [online]. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-.

4.7. European Commission for Democracy Through Law (Venice Commission) (11-12-2016). 106th plenary session [online]. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-PL-PV(2016)001-bil.

4.8. European Commission for Democracy Through Law (Venice Commission) (13-12-2024). *Report on a rule of law and human rights compliant regulation of spyware* [online]. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)043-e.

4.9. Europea Parliament (2015). Mass Surveillance, Part 1 – Risks, Opportunities and Mitigation Strategies, https://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN1)_EN.pdf.

4.10. European Court of Human Rights (2010). Interlaken follow up – Principle of Subsidiarity, note by the Jurisconsult [online]. https://www.echr.coe.int/documents/d/echr/2010_interlaken_follow-up_eng.

4.11. European Court of Human Rights (2012). *Brighton Declaration – High level conference on the future of the European Convention on Human Rights* [online], https://www.echr.coe.int/documents/d/echr/2012_brighton_finaldeclaration_eng.

4.12. European Court of Human Rights (2020). The Rule of Law and the European Court of Human Rights: the independence of the judiciary, Montenegrin Academy of Sciences and Arts, Montenegro, [online], https://www.echr.coe.int/documents/d/echr/Speech_20200228_Sicilianos_Montenegro_ENG.

4.13. European Court of Human Rights (2025). 75 years of the European Convention on Human rights Focus On: The Rule of Law [online], https://ks.echr.coe.int/documents/d/echr-ks/focus-on-the-rule-of-law.

4.14. European Commission for Democracy Through Law (Venice Commission) (15-12-2015). Report on the democratic oversight of signals intelligence agencies [online]. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

4.15. KORFF, Douwe (2013). Note on European & International Law on trans-national surveillance prepared for the civil liberties committee of the European Parliament to assist the Committee in its enquires into USA and European States' surveillance. https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf.

4.16. Open Society Justice Initiative (2012), *Margin of Appreciation: An overview of the Strasbourg Court's margin of appreciation doctrine* [online]. https://www.justiceinitiative.org/uploads/918a3997-3d40-4936-884b-bf8562b9512b/echr-reform-margin-of-appreciation.pdf.

4.17. The European Court of Human Rights ("ECtHR") and the European Union Agency for Fundamental Rights (28-02-2025). *Mass surveillance – ECtHR and CJEU Case-law* [online]. https://fra.europa.eu/sites/default/files/fra_uploads/ecthr-fra-2025-mass-surveillance_en.pdf

SUMMARY

National security as a ground to restrict human rights under the ECHR

Mariami Tchikadze

The present Master's thesis provides an in-depth analysis of the interrelation between national security as a legitimate public interest and the right to privacy under Article 8 of the ECHR in the context of secret surveillance. The right to privacy is a universally recognized human right which prohibits national authorities from unjustifiable interference. At the same time, each state has the primary responsibility to protect everyone within their jurisdiction from national security threats. Balancing these competing interests has a special importance in a democratic society and striking a fair balance between them is impossible without the margin of appreciation doctrine, which is well-established in the ECtHR's case-law.

The thesis examines the essence and main features of the concept of the national security as well as the right to privacy and analyzes how the Court applies the margin of appreciation doctrine in balancing these interests. It compares and analyzes key judgements of the ECtHR on targeted and mass (bulk) surveillance, critically examines the circumstance in which interference in the name of national security was considered justified, and identifying the main factors leading the Court to found that national authorities overstepped their discretion. Due to a detailed analyses of the relevant case-law and materials, the thesis reveals the main factors influencing on the breadth of the margin of appreciation. The author identifies main findings, critically analyzes them and suggest relevant recommendations.

SANTRAUKA

Nacionalinis saugumas kaip pagrindas apriboti žmogaus teises pagal EŽTK

Mariami Tchikadze

Šiame magistro darbe pateikiama išsami nacionalinio saugumo, kaip teisėto viešojo intereso, ir teisės į privatumą pagal EŽTK 8 straipsnį tarpusavio ryšio analizė slapto sekimo kontekste. Teisė į privatumą yra visuotinai pripažinta žmogaus teisė, draudžianti nacionalinės valdžios institucijoms nepagrįstai kištis. Tuo pačiu metu kiekviena valstybė turi pagrindinę pareigą apsaugoti kiekvieną jos jurisdikcijai priklausantį asmenį nuo grėsmių nacionaliniam saugumui. Šių konkuruojančių interesų subalansavimas yra ypač svarbus demokratinėje visuomenėje, o teisingos pusiausvyros tarp jų užtikrinimas neįmanomas be vertinimo ribos doktrinos, kuri yra gerai nusistovėjusi EŽTT praktikoje.

Darbe nagrinėjama nacionalinio saugumo ir teisės į privatumą samprata ir pagrindiniai bruožai, analizuojama, kaip Teismas taiko vertinimo ribos doktriną, derindamas šiuos interesus. Jame lyginami ir analizuojami pagrindiniai EŽTT sprendimai dėl tikslinio ir masinio (masinio) sekimo, kritiškai nagrinėjamos aplinkybės, kuriomis kišimasis nacionalinio saugumo vardu buvo laikomas pateisinamu, ir nustatomi pagrindiniai veiksniai, lėmę Teismą konstatuojant, kad nacionalinės valdžios institucijos viršijo savo diskreciją. Remiantis išsamia atitinkamos teismų praktikos ir medžiagos analize, darbe atskleidžiami pagrindiniai veiksniai, darantys įtaką vertinimo ribos apimčiai. Autorius nustato pagrindinius rezultatus, juos kritiškai analizuoja ir pateikia atitinkamas rekomendacijas.