



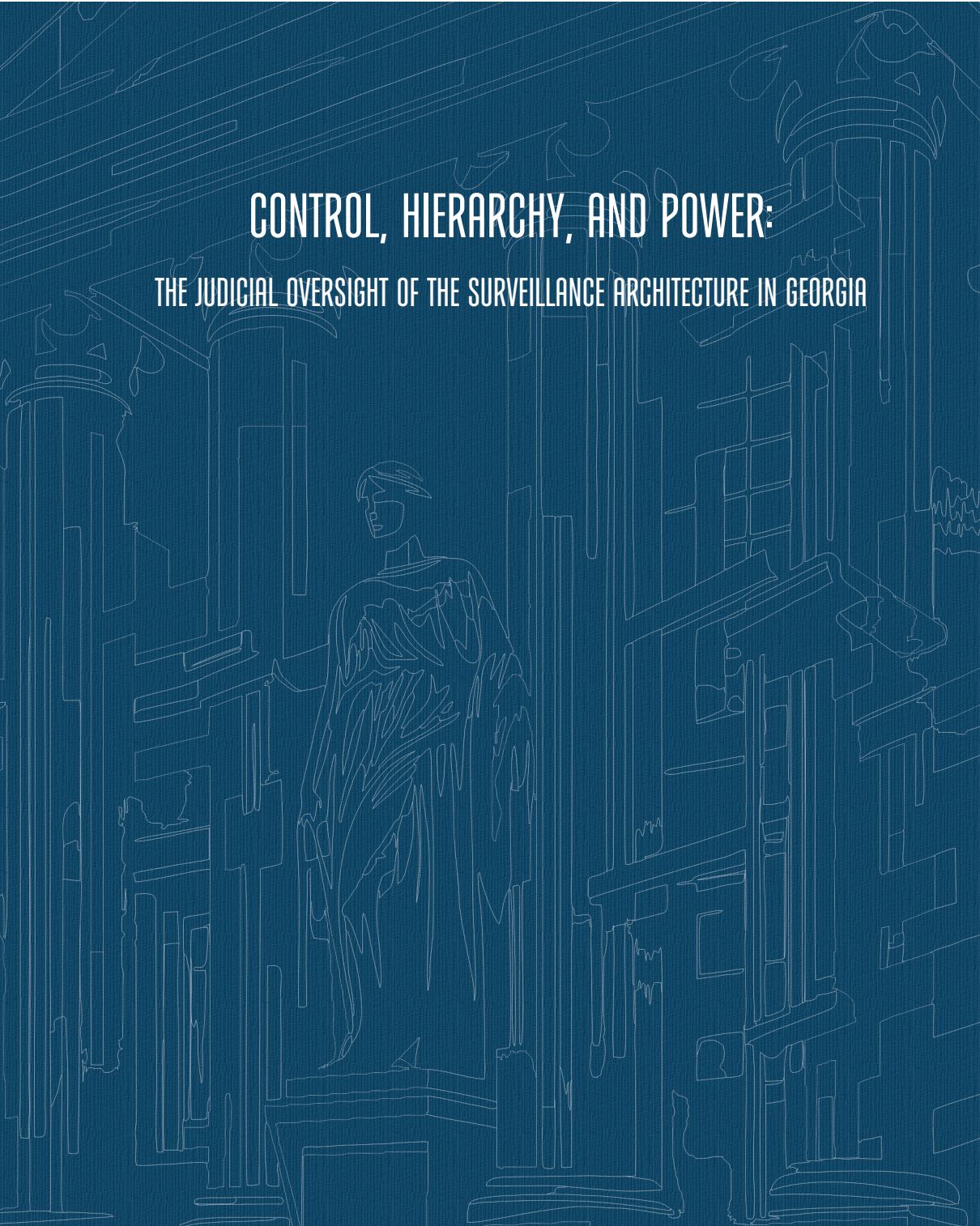
Funded by
the European Union



SOCIAL
JUSTICE
CENTER

CONTROL, HIERARCHY, AND POWER:

THE JUDICIAL OVERSIGHT OF THE SURVEILLANCE ARCHITECTURE IN GEORGIA



**Control, Hierarchy, and Power:
The Judicial Oversight of the Surveillance
Architecture in Georgia**

Social Justice Center
2024



Funded by
the European Union



This publication has been produced with the assistance of the European Union, within the project “Supporting Accountable and Human Rights-oriented Security Sector through Research, Advocacy and Inclusive Dialogue”. Its contents are the sole responsibility of the Social Justice Center and they do not necessarily reflect the views of the European Union.

Responsible Person for the Publication: Guram Imnadze

Researchers: Lia Chkhetiani, Tamta Tsveraidze

Translators: Mariam Begadze, Nino Karanadze

Cover Design: Roland Raiki

Layout Design: Tornike Lordkipanidze

Circulation: 100

ISBN:

It is forbidden to copy, reproduce or distribute the material for commercial purposes without the written consent of the Social Justice Center.

The rule of citation: Social Justice Center, Lia Chkhetiani, Tamta Tsveraidze, “Control, Hierarchy, and Power: The Judicial Oversight of the Surveillance Architecture in Georgia”, 2024.

© Social Justice Center

Address: I. Abashidze 12b, Tbilisi, Georgia

Phone: +995 032 2 23 37 06

www.socialjustice.org.ge

info@socialjustice.org.ge

<https://www.facebook.com/socialjustice.org.ge>

Table of Content

Short Forms and Definitions	7
About the Research.....	10
Methodology.....	14
Chapter 1. Judicial Oversight of the Security Sector’s Use of Surveillance Measures: A Theoretical Perspective	16
1.1 Introduction.....	16
1.2 Why is Judicial Oversight of the Security Sector Necessary?	19
1.3 Practical Limitations of Judicial Oversight.....	21
1.4 Forms of Judicial Oversight	22
1.5 Substantive Scope of Judicial Oversight.....	24
1.6 Transparency of Judicial Oversight.....	27
Chapter 2. Judicial Oversight of Covert Investigative Measures within the Criminal Investigation	29
2.1 Introduction.....	29
2.2 Types of Covert Investigative Measures	29
2.3 Crimes for which the Use of Covert Investigative Measures is Permissible	31
2.4 The Subjects Carrying out Covert Investigative Measures	34
2.5 Targets of Covert Investigative Measures.....	35
2.6 The Procedure for Conducting Covert Investigative Measures and their Control Mechanisms.....	37
2.7 Stages and Terms for Implementation of Covert Investigative Measures	41
2.8 Notification on Covert Investigative Measures and Appeals Mechanisms.....	46
2.9 Familiarization with, Storage and Destruction of Information Obtained as a Result of Covert Investigative Measures.....	49
2.10 Transparency of Judicial Oversight over the Use of Covert Investigative Measures	52
2.11 Trends Identified in Statistical Data	57
2.12 Summary	68

Chapter 3. Judicial Oversight of Special Measures within the Counterintelligence Activities	70
3.1. Introduction.....	70
3.2. Types of Special Measures.....	71
3.3. Agencies Authorized to Conduct Special Measures	76
3.4. Competencies of Special Services and the Problem of Duplication of Powers	77
3.5. Target Objects of Special Measures.....	81
3.6. Procedure for Conducting Special Measures and Judicial Oversight	83
3.7. Problem of Access to Statistical Information	89
3.8. Summary	91
Conclusion	94
Recommendations	96

Short Forms and Definitions

Surveillance Measures – an umbrella term chosen by the authors of the study for stylistic reasons, which refers to all measures of covert surveillance carried out by state bodies for the purpose of investigation and/or counter-intelligence.

Covert Investigative Measures - measures provided for by the Code of Criminal Procedure, which are used for the purpose of investigating a criminal case in the cases foreseen by the Code of Criminal Procedure. Its types are envisaged in Article 143¹ of the Criminal Procedure Code.

Special Measures - operational and operational-technical measures provided for in Article 9 of the “Law on Counterintelligence Activities”, which are used by special state services to carry out counterintelligence activities.

Operational Measures - special measures undertaken in order to obtain information within the framework of counterintelligence activities, which are carried out through overt and/or covert methods. Its types are not defined by law.

Operational-technical Measures - special measures undertaken in order to obtain information within the framework of counter-intelligence activities, which are carried out using technical means. Its types are determined by Article 9, para 2 of the Law on Counterintelligence Activities.

Supervising Judge - a judge of the Supreme Court of Georgia appointed by the chair of the Supreme Court of Georgia, who supervises the implementation of operational-technical measures within the framework of counterintelligence activities.

Trial Judge (Judge) - a judge of the district (city) court, who examines criminal cases in accordance with the territorial jurisdiction and oversees the implementation of covert investigative measures related to the case, in accordance with the procedure provided by the Code of Criminal Procedure.

Operational-Technical Agency (Agency) - a legal entity under public law within the State Security Service (SSSG), which is exclusively authorized to conduct covert investigative measures provided for in subparagraphs “a” - “d”, paragraph 1 of Article 143¹ of the Criminal Procedure Code, Operational-technical measures

provided for in subparagraph “e“, paragraph 2 of Article 9 of counter-intelligence activities, and electronic surveillance measures provided for in paragraph 3 of the same Article.

Special Services – special agencies of the government of Georgia, which carry out counterintelligence activities within the scope of their competence.

Appropriate State Body Carrying Out Covert Investigative Measures - the bodies with the authority to investigate criminal cases in accordance with the territorial jurisdiction under Article 34 of the Criminal Procedure Code and the order of the Prosecutor General are: the Ministry of Internal Affairs (MIA), the Ministry of Defense, the Ministry of Finance, the State Security Service (SSSG), Special Investigation Service and investigators of the Investigative Unit of the Prosecutor’s Office. Accordingly, these bodies have the authority to carry out covert investigative measures that are not exclusively carried out by the operational-technical agency (Article 143¹, subparagraphs “e” and “f”).

State Security Service of Georgia (SSSG) - the appropriate state body carrying out covert investigative measures in the context of criminal investigations; in the context of counterintelligence measures, the SSSG counterintelligence department is responsible for the coordination of counterintelligence activities, and some SSSG structural units are special services carrying out counterintelligence activities.

Ministry of Internal Affairs (MIA) - except for the special rules determined by the order of the Prosecutor General, as a rule, a criminal case belongs to the investigative jurisdiction of MIA investigators. In the context of counterintelligence activities, MIA structural units - General Inspection, Strategic Pipelines Protection Department and Border Police - represent special services.

Prosecutor - the procedural supervisor of investigation in a criminal case, who decides on the initiation, suspension, termination and continuation of covert investigative measures.

Ruling - decision of a district (city) court judge regarding the use of covert investigative measures.

Order - permission from the supervising judge regarding the use of electronic surveillance measures.

Motion - prosecutor's appeal to a district (city) court or supervising judge regarding the use of covert investigative/special measures.

About the Research

Security institutions are a double-edged sword in a democratic state. On the one hand, their effective operation is the guarantee of peaceful and stable development in a country. On the other hand, with weak oversight and lack of accountability, the risk that the surveillance mechanisms at the disposal of security services will become a tool for harassing political opponents and unwarranted interference with human rights increases dramatically. States in the process of democratization are especially vulnerable to such risks, where institutions are not robust enough to contain the power struggles within the rule of law and maintain institutional impartiality. The political processes in the recent years and the increasing involvement of the state security services in them show that Georgia is facing the aforementioned threat and is on the way of becoming a “surveillance state”.¹

The excessive power in the hands of the security sector in Georgia, in particular, the State Security Service (SSSG), is incompatible with the country’s democratic aspirations. Parliamentary and public oversight of the SSSG is weak and its activities are associated with the critical accountability deficit and closure. Cases of mass surveillance of politicians, media, activists and representatives of civil society, blackmailing using personal life and systematic non-investigation of such cases cast doubt on the legality and objectivity of the activities of the SSSG and point to its instrumentalization by the government.

For example, in September 2021, information was spread through the media about 55,000 files allegedly collected by state security services as a result of unlawful surveillance between 2013-2021, the so-called “Krebs” (massive collection of surveillance files), which contained details of personal communications of representatives of civil society organizations, politicians, activists, religious figures, diplomats and journalists.² The recordings, whose authenticity was individually verified by many people, were believed to have been collected by state security services and indicated an established practice of mass surveillance of private communications.³ In 2023, the SSSG itself released secretly obtained video recordings

1 Wegge, N. (2017). Intelligence Oversight and the Security of the State. *International Journal of Intelligence and CounterIntelligence*, 30(4), 687–700.

2 Publika (2021). „Public Defender publishes statement regarding allegedly unlawful surveillance.“ Available at: <https://cutt.ly/sw3a6qMh>. Updated: 28.03.2024.

3 Netgazeti (2022). „19 more journalists request a victim status in the surveillance case.“ Available at: <https://cutt.ly/kw3swehy>. Updated: 28.03.2024.

of lectures and presentations by the civil society organization “Canvas” on forms of nonviolent resistance, which, they claimed, were aimed at organizing “destabilization and civil unrest” by the organization.⁴ Both cases reflect the involvement of politically active groups in the activities of the SSSG and the purpose of influencing public opinion through information operations, which has a large-scale “chilling effect” on the development of democratic processes in the country and essentially worsens the quality of political freedoms.

Essentially, there are two frameworks for using surveillance measures by security services in the country: investigative (law enforcement) and counterintelligence (non-law enforcement). Despite the fact that the activities of security services in these two directions are related to different functions and powers, both are combined in the institutional arrangement of the SSSG in Georgia, which gives this body excessive power and increases the risks of blurring and abusing the powers belonging to different frameworks.

The Constitutional Court drew attention to the risks associated with the investigative functions in the hands of the SSSG in its decision of April 14, 2016, in which it noted that the SSSG “is professionally interested in obtaining as much information as possible,” therefore, the body responsible for investigation should not have technical and Legal control over the means of surveillance.⁵ Despite the fact that the Parliament of Georgia established a new entity - the Operational-Technical Agency - to replace the then unconstitutional surveillance model, it was not granted sufficient institutional guarantees for independence: the agency, as a legal entity under public law (LEPL), remained under the ambit of SSSG governance in law and practice. The presence of investigative functions in the hands of the latter increases the risk of interfering in the agency’s activities and arranging the necessary infrastructure for mass surveillance beyond judicial control.⁶

Given the problematic institutional arrangement of the security sector and weak parliamentary and public oversight, the role of effective judicial supervision in achieving its accountability is particularly important. The assessment of the legali-

4 Social Justice Center (2023). „Total SSSG control continues.“ Available at: <https://cutt.ly/Vw3sexx5>. on 28.03.2024.

5 Decision of the first Chamber of the Constitutional Court of Georgia №1/1/625,640 of April 14, 2016, para 55.

6 Social Justice Center (2017). „Campaign „This Affects You“ statement on an initiative concerning covert surveillance measures.“ Available at: <https://cutt.ly/Iw3su15w>. Updated 28.03.2024.

ty, legitimacy, necessity and proportionality of the use of surveillance mechanisms by alert, effective and competent judges in each individual case ensures that the security services use these mechanisms only when there is an urgent need and in strict compliance with human rights standards.

Only a small part of surveillance (electronic surveillance) carried out within the framework of counterintelligence activities is subject to judicial supervision in Georgia. It is true that the initiation in the case of surveillance for investigative purposes is allowed only with the permission of the court, however, the supervision of the ongoing process is only fragmented and superficial. Statistical data shows that the percentage of authorizations issued by common courts is quite high (more than 80%), which, given the problems of institutional judicial independence, gives impression that judges do not critically evaluate the evidence presented by the security services and are excessively influenced by them.

The need for effective judicial oversight has become particularly evident since the 2022 legislative reform, which dramatically increased the number of articles to which the use of covert investigative measures can be extended. In addition, the time limits for surveillance and notification to citizens have been significantly lengthened, which altogether considerably increased the risks of disproportionate interference with human rights.⁷

The listed factors determine not only the low level of public trust in the security sector (for example, 46% of the population do not think that the SSSG is free from political/party influence⁸), but also have a direct impact on the quality and freedom of activities of media, political and civil groups. In addition, the level of transparency of the activities of the security services is critically low,⁹ which makes it even more difficult to obtain information on the effectiveness of the activities of both the security services themselves and the democratic institutions responsible for its control and supervision. As a result, the public and professional circles have scarce and superficial information about the activities of the security

7 Civil Georgia (2022). Parliament adopted a legislative initiative on covert surveillance measures in a first reading. Available at: <https://civil.ge/ka/archives/487614>. Updated: 28.03.2024.

8 Caucasus Research Resource Center (CRRC), Social Justice Center, Georgian Young Lawyers' Association (2022). Personal and State Security: Public Attitudes and Perceptions 2022, 30. Available at: <https://cutt.ly/jw3svZBf>. Updated: 28.03.2024.

9 Social Justice Center (2023). „Access to Public Information worsens each year“. Available at: <https://cutt.ly/Cw3snvVN>. Updated: 28.03.2024.

services, which has a negative impact on freedoms and personal autonomy, contributes to establishing a feeling of total control in society and mythologizes issues related to the security sphere.

The present study systematically analyzes the degree of democracy, effectiveness and transparency of judicial oversight over the use of surveillance measures by the security services in Georgia and based on it formulates appropriate recommendations for action.

Methodology

The present report aims to analyze the mechanisms of judicial oversight in relation to the surveillance of citizens within the contexts of investigative and counter-intelligence activities. The analysis delineates three distinct phases of oversight over surveillance measures: ex-ante, ongoing, and ex-post facto oversight. Consequently, the principal sources for this research are Chapter XVI¹ of the Criminal Procedure Code (“Covert investigative activities”) and the law of Georgia “On counter-intelligence activities.” While the research will occasionally address the specificities of the institutional arrangements of security services and the various forms of internal and external control, its primary objective is to provide a systematic evaluation of the effectiveness of judicial oversight throughout the process of carrying out surveillance mechanisms. Moreover, the research seeks to assess the democratic nature of this oversight, particularly in terms of its alignment with the principles of checks and balances, accountability, and transparency, as well as its adherence to standards for the protection of fundamental human rights and freedoms.

This document constitutes an empirical doctrinal study utilizing qualitative research methodologies.¹⁰ It is structured into two primary sections. The first section, the theoretical part, delineates the fundamental principles, theoretical caveats, and conceptual elements that a system of judicial oversight over state-sponsored surveillance measures undertaken for investigative and counterintelligence purposes must satisfy. This theoretical framework is grounded in the rationale provided by the European Court of Human Rights in its rulings on the legality of surveillance and the processing of personal data, as well as in scholarly works addressing the legal, socio-political, and ethical dimensions of surveillance. Consequently, the principal methods employed to establish the theoretical framework include a comprehensive review of case law and academic literature.

The second, empirical section of the study examines the institutional framework of judicial oversight concerning citizen surveillance in Georgia and assesses its alignment with the standards of democracy and human rights protection outlined in the theoretical framework. The empirical part of the research is based on the analysis of the legal framework and its practical application.

10 Cane Peter, Kritzer Herbert (2012). *The Oxford Handbook of Empirical Legal Research*, OUP Oxford, 927.

The study of judicial oversight regarding the use of surveillance mechanisms is accompanied by several challenges that impede the comprehensive achievement of research objectives. Primarily, the effectiveness of security services is often intertwined with their secretive nature and a reduced willingness of state agencies to collaborate with civil society, resulting in the lack of publicly available information. This trend has intensified in the recent years in Georgia, with public agencies frequently refraining from providing even the general statistical data, citing the classified nature of such information as a reason.¹¹ Notably, within the research framework, the organization sought public information from the Supreme Court of Georgia, the State Security Service, the Prosecutor's Office, and the Personal Data Protection Service. However, the responses largely reiterated the information already publicly accessible, failed to answer the questions posed, or outright refused to disclose the requested information. Furthermore, the Social Justice Center requested an expert interview with the Operational-Technical Agency's relevant representative, however, did not receive a response. Consequently, a significant limitation of the research was the evident reluctance of the political institutions to share public information and engage in cooperation.

In the initial phase of the research, it was planned to conduct in-depth interviews with individuals possessing professional or personal experience related to the use of surveillance mechanisms. However, during the process of identifying respondents, it became apparent that former or current employees of security services, prosecutors, and judges are reluctant to discuss these topics openly or cite a lack of access to information during the implementation of their duties. Regarding citizens, they are provided with limited information about surveillance activities, and cases of appeals are even rarer. Consequently, the experience of human rights defenders in this area remains limited.

Despite the aforementioned challenges, a systematic analysis of the available sources on legislation and its practical implementation allows for a sufficiently certain assessment of the effectiveness, transparency, and democratic nature of judicial oversight over surveillance bodies. It is important to note that, considering the previously mentioned limitations, this study does not intend to generalize its findings to the entire security sector.

11 Pachulia Tamar (2023). "(Non)Public Information: Impaired Accountability of State Agencies." Social Justice Center. Available at: <https://cutt.ly/iw3s7nlp>. Updated: 28.03.2024.

Chapter 1. Judicial Oversight of the Security Sector's Use of Surveillance Measures: A Theoretical Perspective

1.1 Introduction

Ensuring both internal and external security is a fundamental function of a modern democratic state.¹² Security institutions employ surveillance measures towards citizens as a primary means of fulfilling this role. The interference with human rights through surveillance is an inherent aspect of these institutions' activities, justified by the public objectives of national security, public order, and the protection of the rule of law within a democratic society. The effectiveness of the security sector's operations is closely tied to its flexibility and discretion, with access to modern surveillance technologies enhancing their capabilities, making them particularly powerful and difficult to detect. Under such circumstances, the risks of unwarranted interference with human rights by these bodies significantly increase. Therefore, interference with an individual's right to private and family life through various surveillance mechanisms aligns with the principles of democratic governance only if the basis, scope, and objectives of such intervention are explicitly defined by legislation, adhere to standards of accountability and transparency, and are subject to effective oversight by independent democratic institutions.¹³

In the absence of such oversight, there is a significant likelihood that security services will unlawfully acquire individuals' personal data and utilize it to perpetrate widespread violations of citizens' rights, impose unjustified restrictions on civil and political freedoms, and undermine both formal and informal guarantees of democracy. The absence of effective democratic oversight of the security sector not only unjustifiably expands the scope of these services' activities but also incentivizes political actors with non-democratic

12 European Commission for Democracy through Law (Venice Commission) (2015). Report on the Democratic Oversight of the Security Services, 4. Available at: <https://cutt.ly/tw3fD1lm>. Updated: 28.03.2024.

13 Miyamoto, I. (2020). Surveillance Technology Challenges Political Culture of Democratic States, 49. Available at: <https://cutt.ly/Ew3fKNU8>. Updated: 28.03.2024.

objectives to exert excessive influence over the security sector, using it as a tool to consolidate power.¹⁴

The low level of accountability of security services and the weakness of democratic oversight fosters the risk of an establishment of a “surveillance state”, wherein a significant portion of society, particularly the politically active segment, is subjected to pervasive surveillance. In such societies, as a rule, individual surveillance is typically conducted covertly and remains unnoticed by citizens. Simultaneously, the extensive and comprehensive nature of surveillance is openly acknowledged by the population, as the government systematically utilizes information related to personal life to influence citizens’ behavior and routinely deploys surveillance tools in various domains under broad justifications (for example healthcare, public order, and investigations).¹⁵ Living under constant anticipation of monitored communication channels and physical control impacts both private and public spheres of human activity. This environment fosters a tendency towards self-censorship and excessive caution among citizens, diminishing their inclination to exercise political rights. A daily life characterized by fear and caution contributes to the formation of a politically obedient society, whose passivity depletes democratic institutions and restricts free spaces, thereby creating fertile ground for authoritarian governance.¹⁶

To mitigate these risks, the oversight of security services in a democratic state is conducted by various independent institutions simultaneously. It is preferable that all three branches of government are involved in this process in their distinct capacities.¹⁷

According to the case law of the European Court of Human Rights and the European Court of Justice, it is essential that supervisory institutions maintain both

14 Harfield, C. (2014). Law, morality and the authorization of covert police surveillance. *Australian Journal of Human Rights*, 20(2), 134. Available at: <https://cutt.ly/Ww3fL4cQ>. Updated: 28.03.2024.

15 Elmer, G. (2013). *Panopticon – Discipline – Control*, 25. K. Ball, K.D. Haggerty and D. Lyon, *Routledge Handbook of Surveillance Studies*. New York NY: Routledge.

16 Ball, K., Bellanova, R. and Webster, W. (2019). *Surveillance and democracy: sympathies and antagonisms*, 5. K. Ball and W. Webster, *Surveillance and Democracy in Europe*. New York NY: Routledge.

17 Geneva Centre for the Democratic Control of Armed Forces (2011). *Compilation of Good Practices for Intelligence Agencies and their Oversight*, 23. Available at: <https://cutt.ly/1w3gumTf>. Updated: 28.03.2023.

formal and substantive independence from one another.¹⁸ The scope of democratic oversight by the executive branch is relatively limited, as security services typically fall under the executive branch or are directly subordinate to it. Parliamentary oversight is the primary means of implementing democratic control over the activities of security services, though members of parliament are rarely knowledgeable about the specificities of these activities. Judicial oversight, conducted through systematic and routine examination of individual cases, usually follows instances of interference with citizens' rights by security services. Additionally, quasi-judicial bodies, such as the Personal Data Protection Service, the Ombudsman, and the committee of experts, are involved in supervising specific thematic aspects of the security services' activities.¹⁹

Although the institutional arrangement of the security sector is an integral aspect of a state's sovereign policy and is closely tied to local historical and political context, the case law of the European Court of Human Rights, the 2015 reports of the Venice Commission on democratic oversight of the security sector²⁰ and signal surveillance bodies,²¹ the 2007 Ottawa Principles on Human Rights and Counter-Terrorism,²² the 2013 Tshwane Principles on National Security and the Right to Information,²³ as well as diverse academic literature on the subject offer a general theoretical framework that must be complied with to ensure effective and democratic judicial oversight of citizen surveillance mechanisms.²⁴

For the purposes of this study, surveillance is a set of measures employed by security services to covertly obtain personal data of citizens.

18 Murray, D., Fussey, P., McGregor, L. and Sunkin, M. (2021). Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective. *Journal of National Security Law and Policy*, 753. Available at: <https://cutt.ly/bw3gaHWm>. Updated: 28.03.2023.

19 Compilation of Good Practices for Intelligence Agencies and their Oversight, 23.

20 European Commission for Democracy through Law (Venice Commission) (2015). Report on the Democratic Oversight of the Security Services. Available at: <https://cutt.ly/tw3fD1lm>. Updated: 28.03.2024.

21 European Commission for Democracy through Law (Venice Commission) (2015). Report on the Democratic Oversight of Signals Intelligence Agencies. Available at: <https://cutt.ly/bw3gaHWm>. Updated: 28.03.2024.

22 University of Ottawa Faculty of Law (2007). Ottawa Principles on Anti-terrorism and Human Rights. Available at: <https://cutt.ly/ow3gbG0t>. Updated: 28.03.2024.

23 The Global Principles on National Security and the Right to Information (The Tshwane Principles) (2013). Available at: <https://cutt.ly/Qw3gQpTM>. Updated: 28.03.2024.

24 Report on the Democratic Oversight of the Security Services, 7.

1.2 Why is Judicial Oversight of the Security Sector Necessary?

Surveillance conducted by security services may serve both investigative and counterintelligence purposes.²⁵ The former is typically carried out by investigative agencies (such as the police) to investigate crimes, while the latter is performed by counterintelligence services to safeguard the country's internal security (for example, against threats like terrorism, extremism, and hybrid warfare).²⁶ Investigative surveillance targets specific individuals or groups suspected of criminal activity, whereas counterintelligence surveillance may not have a clearly identified target group and serves "strategic" purposes. This means the basis for such surveillance extends beyond the risk of a particular crime or threat to proactive collection of relevant information enabling the broader security, strategic, and foreign policy determination.²⁷

In practice, only investigative surveillance is routinely subjected to judicial oversight, while the activities of counterintelligence services are controlled by the courts indirectly or only in specific cases.²⁸ This difference arises from the political nature of counterintelligence activity, which, unlike criminal activity, does not necessarily involve a specific judicial process. While it is permissible for counterintelligence agencies to operate with a greater degree of secrecy and flexibility, extending judicial oversight to their activities is essential to maintain legitimacy and legality. Security services inherently tend to gather "as much"²⁹ information as possible. The requirement to obtain court permission for surveillance or subsequently verify the legality of the obtained information encourages self-restraint within the security services and serves a preventive function, as they must meet a minimum standard of justification to convince a judge. Consequently, counterintelligence services will have to employ surveillance mechanisms only when it is necessary and as a last resort to achieve national security objectives.

25 Ibid, 23.

26 Malgieri, G. and De Hert, P. (2017). European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably but Not Necessarily by Judges, 518. D. Gray and S. E. Henderson, eds., *The Cambridge Handbook of Surveillance Law*. New York, NY: Cambridge University Press.

27 Report on the Democratic Oversight of Signals Intelligence Agencies, 3.

28 European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges, 518.

29 Report on the Democratic Oversight of the Security Services, 13.

According to the case law established by the European Court of Human Rights in the precedential cases “Szabo and Vissy v. Hungary” and “Klass and Others v. Germany,” judicial oversight should be extended to all types of surveillance and be conducted by judges with specialized expertise.³⁰ In *Klass and Others v. Germany*, the Court emphasized that the rule of law necessitates effective judicial checks on executive interference with human rights, at least as a last resort remedy, because “judicial oversight offers the best guarantees of independence, impartiality, and due process protection.”³¹ In another landmark decision, *Big Brother Watch and others v. the United Kingdom*, the European Court reiterated the desirability of having a judicial authority at the helm of a security sector oversight system, whose decisions would be binding.³² Additionally, judicial oversight provides an opportunity to identify gaps in the legislation, thereby giving the parliament an impetus to enhance the legislative framework.³³

The necessity for judicial oversight in the field of security also arises from the fact that, unlike the parliament and executive power, the court is not a political body, is not involved in daily political processes and is therefore less subject to the influence of public opinion or political interests.³⁴ This impartiality is particularly relevant during crises, when both executive and parliamentary authorities feel public pressure and consequently strive to take effective steps within a short period. Unlike these branches of government, the judiciary can impartially evaluate the compliance of security services’ activities with human rights standards with a “cold mind” adhering to professional standards, all while operating under conditions of relative freedom from political pressure.³⁵

Thus, within the framework of judicial oversight, it is possible to assess both the formal legality of initiating surveillance and its substantive compliance with constitutional norms and human rights standards.

30 Report on the Democratic Oversight of the Security Services, p. 13.

Case of *Szabo and Vissy v. Hungary*. 37138/14, 40-41. European Court of Human Rights (2016).

31 Case of *Klass and Others v. Germany*. 5029/71, 55. European Court of Human Rights (1978).

32 Case of *Big Brother Watch and Others v. the United Kingdom*, 58170/13, 62322/14, 24960/15, 320. European Court of Human Rights (2021).

33 McIntyre, T.J. (2015). *Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective*, 144. Available at: <https://cutt.ly/Jw3vpUVA>. Updated: 28.03.2024.

34 Office of the High Commissioner for Human Rights (2021). *The Right to Privacy in the Digital Age: Report*, 14. Available at: <https://cutt.ly/Tw3vsfN>. Updated: 28.03.2024.

35 *Judicial Oversight of surveillance: the case of Ireland in comparative perspective*, 139.

1.3 Practical Limitations of Judicial Oversight

It should be noted that judicial oversight of the use of surveillance mechanisms does not, in itself, guarantee effective democratic control, as judges often grant surveillance permissions automatically and rarely investigate the actual grounds for their necessity.³⁶ The effectiveness of surveillance is compromised by various limitations, which must be addressed to ensure that the court is equipped with the necessary tools to verify the legality of surveillance.

At the initial, authorization stage of surveillance, information is often presented to the court partially, solely from the perspective of the security services. At this stage, the absence of the principle of adversariality and the binary relationship between the court and the security services, which excludes the potentially differing position of a citizen or another supervisory body, creates a risk that a judge may refrain from thoroughly investigating the activities of the security services, rely excessively on their justifications, and be overly cautious about the security risks they highlight, leading to an increased likelihood of issuing permissions to initiate surveillance.³⁷ In such instances, judicial oversight becomes merely a formal procedure, contributing to the development of the security sphere as a “state within a state”.³⁸ Therefore, as articulated in Tshwane’s 2013 principles, it is desirable that the content of security risks be more precisely defined by legislation and that judges be equipped with the practical knowledge and skills necessary to thoroughly assess the appropriateness of security services’ activities and ensure compliance with human rights and democratic principles in implementing surveillance measures.³⁹

Furthermore, given the rapid advancement of surveillance technologies, judges may lack the specialized knowledge necessary to effectively assess the true extent and scope of surveillance.⁴⁰ In criminal proceedings, in which evidence obtained through surveillance is subject to evaluation by the other party, there is a possibility that a judge, upon a defendant’s direction, will more critically examine the content, form, and legality of the obtained evidence at sub-

36 The Right to Privacy in the Digital Age, 13.

37 Judicial Oversight of surveillance: the case of Ireland in comparative perspective, 127.

38 Report on the Democratic Oversight of the Security Services, 17.

39 The Tshwane Principles, 4.

40 Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective, 749.

sequent stages of granting surveillance permission. In contrast, information gathered during counterintelligence activities, much of which is collected for “strategic” and “research” interests, is relatively rarely subjected to detailed scrutiny. Even in such cases, the effectiveness of such scrutiny depends significantly on the judge’s technical skills and in-depth understanding of the security context. To mitigate this risk, some countries, such as Canada, France, Spain, the United States, and South Africa, have specialized judges to hear cases related to counterintelligence.⁴¹ However, this approach may result in isolating specialized judges from other types of cases and establishing a permanent working relationship with security bodies, which carries the risk of “institutional capture”⁴² – where the supervisory body begins to identify with the institution it oversees and adopts its institutional “mentality.”⁴³ Therefore, it is desirable to involve quasi-judicial bodies with technical expertise in the judicial oversight process, providing assistance to non-specialized judges, or to rotate specialized judges and involve them in other types of cases.

1.4 Forms of Judicial Oversight

Judicial oversight of surveillance measures can be carried out in three ways. These forms are:

- (1) Ex ante oversight, which involves giving permission to use surveillance mechanisms;
- (2) Ongoing oversight, which includes monitoring the progress of surveillance;
- (3) Ex post oversight, which involves verifying the legality of surveillance after its completion.⁴⁴

At all three stages, the security services are accountable to the judge assigned to an individual case. This entails their obligation to provide explanations of their activities to the supervisory body, and if necessary, to assume responsi-

41 Born, H. and Wills, A. (2021). *Overseeing Intelligence Services: A Toolkit*, 96. Available at: <https://cutt.ly/Kw3vIutn>. Updated: 28.03.2024.

42 Venice Commission Report on the Democratic Oversight of the Security Services, 13.

43 Mitnick, B.M. (2011). *Capturing ‘Capture’: Definition and Mechanisms*, 36. Available at: <https://cutt.ly/tw3vOhFv>. Updated: 28.03.2024.

44 Venice Commission Report of the Democratic Oversight of the Security Services, 16.

bility for the resulting consequences, and accept the liability in the event of mistakes.⁴⁵

A form of *ex ante* control involves granting permission to initiate surveillance. During this phase, a judge examines the legal and factual grounds for surveillance and issues a decision in the form of a relevant document. Oversight during the course of surveillance (ongoing oversight) involves addressing complaints submitted by citizens who have become aware of the surveillance. However, this is a relatively rare occurrence and renders judicial oversight largely reactive.⁴⁶ Therefore, to implement effective supervision at this stage, it is desirable for the court to have the authority to proactively monitor the surveillance process through methods such as random case selection, unplanned investigative visits, thematic investigations, and other forms of oversight. *Ex-post* oversight can be conducted by assessing the legality of the obtained evidence during the criminal proceedings and by reviewing its appropriateness after the surveillance has concluded.

In the case of *Uzun v. Germany*, the European Commission for Human Rights emphasized that the court's authority to declare evidence obtained through surveillance inadmissible is a crucial oversight mechanism, albeit applicable only to surveillance conducted for investigative purposes.⁴⁷ Another significant aspect of *ex post* oversight is the requirement for security services to notify citizens within a specified period after surveillance concludes.⁴⁸ Following notification, citizens have the opportunity to challenge the legality of the surveillance in court and seek compensation for damages. Due to frequent non-compliance with the notification obligation by security services, judicial oversight is essential to ensure both the fulfillment of notification requirements and proactive verification of the legality of completed surveillance, since it is expected that even in the case of notification, citizens will rarely exercise this right due to the relatively secretive and closed nature of the security services.⁴⁹

45 *Ibid*

46 Effective Oversight of large-scale surveillance activities, 759.

47 Case of *Uzun v. Germany*. 35623/05, 80. European Court of Human Rights (2010).

48 Ohm, P. (2017). *The Surveillance Regulation Toolkit: Thinking beyond Probable Cause*, D. Gray and S. E. Henderson. *The Cambridge Handbook of Surveillance Law*. New York, NY: Cambridge University Press.

49 Eskens, S., Daalen, O. van and van Eijk, N. (2015). *Ten standards for oversight and transparency of national intelligence services*. Institute for Information Law at the University of Amsterdam, 27. Available at: <https://cutt.ly/rw3vJ9LH>. Updated: 28.03.2024.

According to the case law of the European Court of Human Rights, judicial oversight, particularly in cases of extensive “strategic” surveillance, should encompass all phases of the surveillance process. Consequently, the judiciary should exercise supervision over all three stages, including oversight over technical aspects such as the selection of surveillance targets, the establishment of criteria for categorizing acquired information, and the filtering of information based on these criteria.⁵⁰

During the authorization and subsequent oversight phases, it is crucial for the legislation to acknowledge the inherent risks associated with having the same judge oversee the entire surveillance process. A judge who grants authorization for surveillance tends to be less inclined to critically reassess own initial decision when evaluating the proportionality of surveillance during later stages of supervision. Some researchers argue that the authorizing judge tends to “mark their own homework” during subsequent oversight phases.⁵¹ Therefore, the likelihood of achieving a thorough evaluation may increase if different judges handle the authorization, monitoring, and ex post phases. However, the advantage of a single-judge oversight model lies in the judge’s familiarity about the surveillance process as a whole enabling a comprehensive understanding of the case nuances and decisions that are informed by case-specific contexts.⁵²

1.5 Substantive Scope of Judicial Oversight

According to the Ottawa Principles, oversight of the security sector should ensure the validity, efficiency, transparency, legality, and accountability of its activities.⁵³ An essential prerequisite for effective oversight of the use of surveillance mechanisms is that the grounds for interference in an individual’s personal and family life are defined by legislation and meet the minimum requirements of foreseeability. This condition derives from Articles 8 and 13 of the European Convention on Human Rights. According to Article 8, Part 2, interference in private and family life is permissible “in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights

50 Case of Big Brother Watch and Others v. the United Kingdom, 58170/13, 62322/14, 24960/15, 320. European Court of Human Rights (2021).

51 Venice Commission Report on the Democratic Oversight of the Security Services, 4.

52 Judicial Oversight of surveillance: the case of Ireland in comparative perspective, 142.

53 Ottawa Principles on Anti-terrorism and Human Rights, 7.

and freedoms of others⁵⁴ Article 13 guarantees the right to “an effective remedy” in response to violations of fundamental rights.⁵⁵ Considering best practices of judicial oversight, legislation should clearly define:

- Objectives, terms and mechanisms of information collection;
- The circle of people whose data can potentially be collected (for example, it is a good practice to limit the collection of information related to the activities of special circles - journalists, lawyers and clergymen);⁵⁶
- The minimum standard of justification for interference with rights;
- Procedures for authorizing the use of surveillance measures, monitoring the progress of their use, and reviewing their necessity after conclusion or based on citizen’s complaints.⁵⁷

Legislation should also specify the emergency situations under which security services are authorized to initiate surveillance without prior judicial approval, subject to subsequent judicial review. Clarity and comprehensiveness in legislation help mitigate risks of selective interference with human rights and the potential “chilling effect” of surveillance of citizens.⁵⁸ For instance, in cases such as “Weber and Saravia v. Germany” and “Huvig v. France”, the European Court of Human Rights established the minimum criteria for wiretapping that any foreseeable legislative framework must adhere to:

- The range of crimes for which the use of wiretapping is permitted;
- The duty of judges to clearly define the limited categories of citizens who may be subject to covert surveillance in their decisions;
- Maximum duration and limitations of wiretapping;
- The procedures for processing, using and storing the obtained data;
- Precautionary measures undertaken in the case of data sharing with third parties;
- The cases, in which data must be erased or records be destroyed.⁵⁹

54 Council of Europe (1950). European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8.

55 Ibid, Article 13.

56 Compilation of Good Practices for Intelligence Agencies and their Oversight, 23.

57 Ibid, 12.

58 Report on the Democratic Oversight of the Security Services, 25.

59 Case of Weber and Saravia v. Germany, 54934/00, 94. European Court of Human Rights (2006). Case of Huvig v. France, 11105/84. European Court of Human Rights (1990). European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards ‘Good Enough’ Oversight, Preferably but Not Necessarily by Judges, 513.

The legislative provision should also provide for the exhaustive list of surveillance measures and provisions for restoring rights to citizens in the case of unlawful surveillance.⁶⁰ A clear and thorough legal framework enables judges to accurately and systematically assess the alignment of arguments and factual evidence presented by security services with the law. Moreover, when overseeing the surveillance process, judges should adopt an impact and risk assessment approach, evaluating the extent to which the surveillance measures uphold standards of necessity and proportionality. In each case, judges must consider the potential impact of surveillance on human rights and democratic processes, requiring security services to substantiate that the use of surveillance measures is indispensable for achieving the security objectives in their justifications.⁶¹

In practice, the justification standard for employing surveillance mechanisms typically is reasonable doubt, probable cause, or even - relevance of the matter.⁶² In other words, to secure court authorization to conduct surveillance over a citizen, security services are obligated to justify the need only to this minimal level. Given the modern means of communication and the presence of sophisticated surveillance technologies, which can be deployed economically, this standard of justification often enables security services to gain comprehensive access to individuals' communication channels (such as computers or mobile memory cards) and simultaneously gather information unrelated to the case.⁶³ Leveraging extensive technical capabilities, security services frequently operate under the principle of "looking for a needle in a haystack," amassing vast amounts of data from communication channels and subsequently filtering through information repositories based on specific criteria relevant to the case.⁶⁴ Consequently, some scholars argue that as citizen mass surveillance becomes technically easier, courts should more rigorously oversee the scope of security services' activities.⁶⁵ Therefore, the standard for justifying the collection of personal information must be stringent, adhering closely to the accuracy standards established in the jurisprudence of the European Court of Human Rights. Furthermore, the level of scrutiny should in-

60 Ten standards for oversight and transparency of national intelligence services, 28.

61 *Ibid*, 29.

62 The Surveillance Regulation Toolkit: Thinking beyond probable cause, 491.

63 Brown, I., Halperin, M.H., Hayes, B., Scott, B. and Vermeulen, M. (2015). Towards Multilateral Standards for Surveillance Reform, 2. Available at: <https://cutt.ly/6w3bdowt>. Updated: 28.03.2024.

64 *Ibid*

65 *Ibid*

crease when justifying the need for ongoing surveillance. Moreover, when authorizing surveillance, judges should apply the principle of minimization, specifying precisely what types of data security services may collect and how excess information should be disposed of. Judicial oversight should also ensure that surveillance measures are employed as a last resort to achieve investigative objectives.⁶⁶

To conduct meaningful oversight, it is crucial that the court has unrestricted access to all pertinent materials throughout the entire oversight process. In a 2015 report, the Council of Europe's Commissioner for Human Rights underscored that legislation should ensure supervisory institutions' access to all forms of information, "regardless of their degree of secrecy," including by empowering courts with investigative functions.⁶⁷ Additionally, security services are obliged to maintain an "open and cooperative" approach towards supervisory authorities.⁶⁸ For this right to be effectively exercised, it is imperative that security services maintain meticulously detailed and accurate records of their activities in an accessible format, enabling courts to verify this information when necessary.⁶⁹

Judicial oversight also extends to the management of information acquired by security services. The court should scrutinize whether the security services verify the relevance and accuracy of the obtained information and ensure that incorrect or irrelevant information is promptly deleted or destroyed in accordance with the established procedures.⁷⁰

1.6 Transparency of Judicial Oversight

The democratic nature of judicial oversight is not solely defined by the effectiveness of oversight over security services. The court also has an obligation to provide the public with adequate information regarding the progress of surveillance and the outcomes of its oversight, as well as to ensure meaningful engagement of

66 The Surveillance Regulation Toolkit: Thinking beyond probable cause, 494.

67 Council of Europe Commissioner for Human Rights (2015). Democratic and effective oversight of national security services, 13. Available at: <https://cutt.ly/ww3bz3lv>. Updated: 28.03.2024.

68 Ibid

69 Ibid, 8.

70 Compilation of Good Practices for Intelligence Agencies and their Oversight, 25.

citizens and civil society.⁷¹ This can be achieved, for instance, by proactively publishing surveillance methodologies, periodic reports, aggregated statistical data, results of thematic investigations, and similar information.⁷²

The degree of transparency and accessibility of the judiciary plays a critical role in fostering public trust, sense of fairness, and security both within the judiciary and security services. The primary guiding principle for both judicial oversight and activities of security services should be transparency, with secrecy reserved as an exceptional measure applicable solely to highly sensitive security matters. Legislation should precisely and comprehensively define the nature of classified information.⁷³

Even in cases involving classified information, both judicial authorities and security services have the capacity to disclose reasonably detailed information to the public, for instance, through encryption of strategic details or after the conclusion of operational activities. The right of citizens to access information obliges the state to clearly define in legislation the circumstances under which information may be kept confidential on grounds of national security. In each instance, both the judiciary and security services must clearly justify the need for imposing such restrictions.⁷⁴

71 Effective Oversight of large-scale surveillance activities, 752.

72 Ten Standards for oversight and transparency on national intelligence services, 28.

73 Effective Oversight of large-scale surveillance activities, 743.

74 The Tshwane Principles, 6.

Chapter 2. Judicial Oversight of Covert Investigative Measures within the Criminal Investigation

2.1 Introduction

As discussed in the first chapter, surveillance measures serve both investigative and counterintelligence purposes. In the context of investigations, surveillance typically focuses on a specific crime and a limited group of individuals associated with it, with the primary aim of gathering evidence for a particular trial. In contrast, as a rule, in counterintelligence context, surveillance mechanisms are not tied to any specific crime. Instead, they involve the proactive collection of information concerning risks pertinent to national security. Although both types of surveillance activities should be subject to judicial oversight, their political and legal natures differ significantly. Consequently, this study examines investigative and counterintelligence regimes separately.

This chapter addresses the use of various surveillance measures for criminal purposes, referred to in the Criminal Procedure Code as “covert investigative measures”. This section of the study will examine the legislation that defines judicial oversight of covert investigative measures, primarily detailed in Chapter XVI¹ of the Criminal Procedure Code. The subsequent chapter will focus on the legislation governing judicial oversight of special measures for obtaining information through technical means for counterintelligence purposes, as primarily outlined in the Law on “Counterintelligence Activities”.

2.2 Types of Covert Investigative Measures

The Criminal Procedure Code defines an exhaustive list of covert investigative measures, restricting investigative bodies to the use of only those mechanisms explicitly defined by law for law enforcement purposes.⁷⁵ In light of the rapid advancement of surveillance technologies, it is crucial for legislation to ensure a high standard of foreseeability. This allows citizens to determine in advance the

⁷⁵ Criminal Procedure Code, Article 1432, Part 2.

forms in which law enforcement agencies may monitor their private lives and communications.

The legislation defines the following six types of covert investigative measures:

- the covert wiretapping and recording of telephone communications;
- the retrieval and recording of information from a communications channel and the computer system, which also includes installation of respective software in the computer system for this purpose;
- real-time geolocation identification;
- the monitoring of postal and telegraphic transfers;
- covert video and/or audio recording, photographing;
- electronic surveillance.⁷⁶

The Criminal Procedure Code provides detailed definitions for some of the listed mechanisms. Specifically, **covert wiretapping** is defined as the secret surveillance and recording of telephone communications conducted through the electronic communication networks and facilities of an authorized company.⁷⁷ **The retrieval and recording of information from communication channels** involve the removal and recording of current, transmitted, received, collected, processed, or accumulated information from electronic communications (e.g. email), communication networks, telecommunication, or information systems by an authorized body using technical and/or software means.⁷⁸ Similarly, **the retrieval and recording of information from computer systems** refer to the removal and recording of information transmitted, received, collected, processed, or accumulated within a computer system by an authorized body using technical and/or software means.⁷⁹ **Real-time geolocation identification** is defined as the determination of the geographical location of mobile communication equipment in real-time with the highest possible accuracy.⁸⁰

76 Ibid

77 Ibid, Article 3, Part 36.

78 Ibid, Part 33.

79 Ibid, Part 34.

80 Ibid, Part 35.

The legislation does not define certain covert investigative measures, such as **the monitoring of postal and telegraphic transfers, covert video-audio recording and photographing, and electronic surveillance by technical means**. While the nature of the first two measures is relatively comprehensible to the general public, the specificities of electronic surveillance remain ambiguous. It is unclear how this type of surveillance differs from other covert investigative measures or visual monitoring provided for operational-search measures, both of which can also be conducted using technical means.⁸¹

It is noteworthy that in 2023, the Public Defender of Georgia filed a lawsuit with the Constitutional Court, seeking to declare the use of visual surveillance without a court decision unconstitutional.⁸² One of the principal arguments presented by the claimant was that visual surveillance can be conducted electronically, making it „similar to one of the measures used in covert investigative activities – electronic tracking“.⁸³ Consequently, the practical distinction between visual surveillance and electronic tracking is blurred. Clarifying what this distinction entails and defining electronic surveillance in the Criminal Code is crucial for the proper protection of human rights. According to the legislation, electronic surveillance as a form of covert investigative activity must be subject to judicial oversight. In contrast, visual surveillance, which is an operational-search measure, is not subject to judicial supervision.

2.3 Crimes for which the Use of Covert Investigative Measures is Permissible

The Criminal Procedure Code outlines an exhaustive list of cases, during the investigation of which the use of covert investigative measures is permissible. Before the legal reform of June 2022,⁸⁴ the scope of covert investigative measures was primarily limited to intentional serious and especially serious crimes, along with a limited number of less serious offenses. However, the reform expanded this list

81 Law of Georgia “On Operational Search Activities”, Article 1, Section 2, Subsection “c”.

82 “The Public Defender of Georgia against the Parliament of Georgia”, N1/1/1630, Constitutional Court of Georgia (2023). Available at: <https://constcourt.ge/ka/judicial-acts?legal=14894>. Updated: 28.03.2024.

83 Ibid

84 Civil Georgia (2022). “Venice Commission Criticizes Changes to Covert Investigations.” Available at: <https://civil.ge/ka/archives/506293>. Updated: 28.03.2024.

to include the 27 additional less serious crimes from various chapters of the Criminal Code.⁸⁵

It should be noted that these changes have sparked significant criticism. Local non-governmental organizations jointly urged the President of Georgia to veto the draft law, arguing that it considerably deteriorated the standard of human rights protection during the implementation of covert investigative measures.⁸⁶ The President did exercise the veto power, emphasizing that during Georgia's candidacy for EU membership, such a law unjustifiably restricting human rights should not have been adopted.⁸⁷ The then Ambassador of the European Union to Georgia, Karl Hartzel, remarked that these changes significantly infringed upon the privacy of Georgian citizens.⁸⁸

According to the opinion of the Venice Commission, the explanatory note accompanying the legislative initiative cited only general purposes, such as the prevention of terrorism, the threat of hybrid warfare, and organized crime, as the rationale for expanding the scope of covert investigative activities. The explanatory note did not adequately justify why these changes – and the resulting ex-

85 Crimes that create a threat to human life and health (XXI), are directed against sexual freedom and inviolability (XXII), against human rights and freedoms (XXIII), against property (XXV), against entrepreneurial or other economic activities (XXVI), against the monetary-credit system (XXVII), against public security and order (XXX), against public health and morality (XXXII), against cultural heritage (XXXIII), related to narcotics (XXXIV), cybercrime (XXXV), against environmental protection (XXXVI), against the constitutional order and security foundations (XXXVII), violations of the legal regime of the occupied territories (XXXVIII), terrorism (XXXIX), against the rule of government (XL), and against humanity (XLVII) are categorized as follows. Additionally, all forms of official crimes (XXXIX) fall under this classification.

According to Article 12 of the Criminal Code, crimes are classified into three categories: less serious, serious, and especially serious. A less serious crime is an intentional or negligent offense for which the maximum punishment does not exceed five years of imprisonment. A serious crime is defined as an intentional offense for which the maximum penalty does not exceed ten years of imprisonment, or a negligent crime for which the maximum penalty is more than five years of imprisonment. An especially serious crime is an intentional offense for which the punishment exceeds ten years of imprisonment or includes a life sentence.

86 Transparency International Georgia (2022). "We call on the President to veto the worsened surveillance legislation." Available at: <https://cutt.ly/pw3npNxM>. Updated: 28.03.2024.

87 Civil Georgia (2022). "President Vetoes Bill on Covert Investigative Measures." Available at: <https://cutt.ly/pw3na6Wk>. Updated: 28.03.2024.

88 Delegation of the European Union to Georgia (2022). „Remarks by Ambassador Carl Hartzel following the amendments to the criminal procedure code.“ Available at: <https://cutt.ly/jw3nsnvh>. Updated: 28.03.2024.

tensive interference with human rights – were necessary, especially considering that the newly added crimes were mostly categorized as less serious ones.⁸⁹ The Commission also pointed out that the changes were not supported by actual data.⁹⁰ Furthermore, the Legislature did not assess the inherent risks to human rights posed by these changes, nor did it consider the availability of other, less restrictive alternatives.⁹¹

According to the principles governing the use of covert investigative measures as defined by the Criminal Procedure Code, surveillance measures must be related not only to formally enumerated crimes but must also serve legitimate purposes in a democratic society. These purposes include ensuring national security or public safety, preventing disorder or crime, promoting economic well-being, or protecting the rights and freedoms of others.⁹² Additionally, the use of covert investigative measures must be necessary, urgent, proportionate, and a last resort, employed only when evidence cannot be obtained by other means or would require an unjustifiably large effort.⁹³ The 2022 legislative changes, which expanded the scope of covert investigative measures to include a broader range of crimes, increase the risk of human rights violations and arbitrariness. This expansion contradicts the principles set forth in the Criminal Procedure Code, as it transforms covert investigative measures from special measures into ordinary investigative mechanisms.

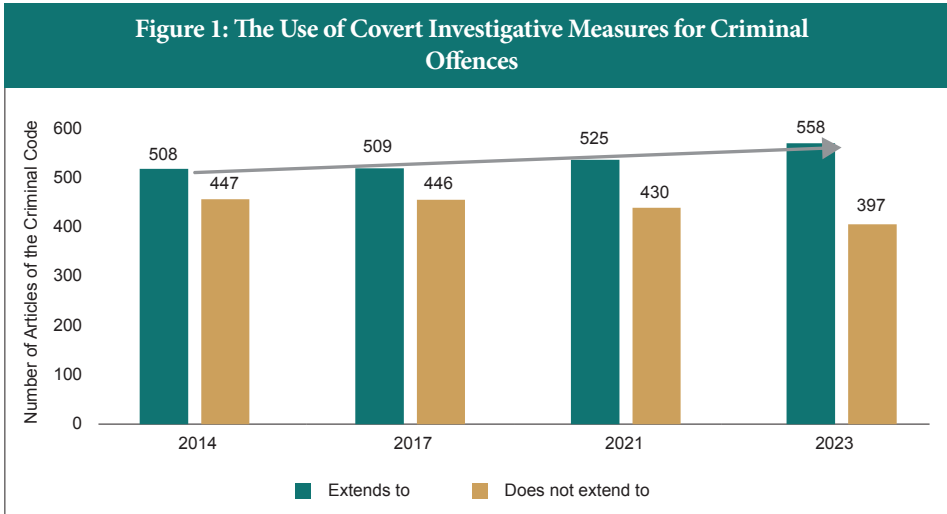
89 European Commission for Democracy through Law (Venice Commission) (2022). Georgia - Urgent opinion on the Draft Law on the Amendments to the Criminal Procedure Code adopted by the Parliament of Georgia on 7 June 2022, 8. Available at: <https://cutt.ly/Mw3nfxmR>. Updated: 28.03.2024.

90 Ibid, 9.

91 Ibid

92 Criminal Procedure Code, Article 1432 Part 2.

93 Ibid, Part 3 and 4.



Thus, as a consequence of the 2022 reform, covert investigative measures have been extended to a broader spectrum of crimes. These crimes vary significantly in terms of their severity, the nature of the wrongful activities involved, the perpetrators, and the objects of criminal protection.

2.4 The Subjects Carrying out Covert Investigative Measures

During the investigative process, a prosecutor makes decisions regarding the execution of covert investigative measures.⁹⁴ The exclusive authority to conduct covert investigative measures (e.g. covert wiretapping and recording of telephone communications, extraction and fixation of information from communication channels and computer systems, real-time geolocation determination, and control of postal and telegraphic transfers), as stipulated in subsections “a” to “d” of part 1 of Article 143¹, rests with the operational-technical agency under the prosecutor’s instructions.⁹⁵ In contrast, other covert investigative measures (including covert video recording, covert audio recording, photographing, and electronic tracking by technical means) can be conducted by the relevant state body authorized to carry out such measures within their respective competence.⁹⁶ These

94 Criminal Procedure Code, Article 143³ Part 1.

95 Criminal Procedure Code, Article 3, Part 32, Subsection „a“.

96 Ibid, Subsection „b“.

bodies include the Ministry of Justice, the Ministry of Internal Affairs, the Ministry of Defense, the Ministry of Finance, the State Security Service, the Special Investigation Service, and the Prosecutor's Office.⁹⁷ The distribution of investigative responsibilities among these bodies is regulated by the order of the Prosecutor General of Georgia.⁹⁸ Consequently, within the scope of their professional powers, the investigators of these bodies are authorized to carry out those covert investigative measures that do not fall under the exclusive purview of the operational-technical agency.

It should be noted that this reasoning derives from a systematic interpretation of the pertinent articles of the Criminal Procedure Code, since the legislation employs a vague and general term, "the relevant state body carrying out covert investigative measures within the scope of its competence". The legislation concerning surveillance should be exceptionally clear, specific, and comprehensible to the general public. Therefore, instead of using general terminology, the Code should explicitly identify the authorities entitled to conduct covert video and audio recording, photographing, and electronic tracking.

2.5 Targets of Covert Investigative Measures

Covert investigative measures can be used in the cases mentioned above during the ongoing investigation and criminal prosecution of a "person directly connected to the crime". This term refers to individuals who are reasonably suspected of having committed any of the crimes defined by law, for which the use of covert investigative measures are permitted.⁹⁹ Additionally, covert investigative measures can be employed against individuals who are in direct communication with a "person directly connected with the crime" – specifically, those who receive or transmit information intended for or provided by, a person directly connected with the crime, or those whose means of communication are used by the person directly connected with the crime.¹⁰⁰

97 Criminal Procedure Code, Article 34.

98 Prosecutor General of Georgia, order No. 3 "On determination of investigative and territorial investigative jurisdiction of criminal law cases," August 23, 2019. Available at: <https://cutt.ly/Pw3nk0As>. Updated: 28.03.2024.

99 Criminal Procedure Code, Article 143³ Part 2, Subsection „b“.

100 Ibid

Thus, covert investigative measures can potentially be used by the authorities against any citizen who potentially provides or receives information from an alleged suspect or uses his or her means of communication. It is unclear as to whether the standard of “reasonable doubt”¹⁰¹ applied to the alleged defendant also applies to other persons related to him. Thus, under the conditions of bad faith use, there is a risk that covert investigative measures with the argument of a possible connection with the alleged accused will be extended to a fairly wide circle of people. Accordingly, courts should evaluate the factual circumstances especially carefully and critically in the event that surveillance is planned for other, presumably innocent, persons in communication with the alleged criminal. When meeting the standard of reasonable doubt about the alleged guilt of a “person connected with the crime”, using the same standard, a prosecutor must additionally substantiate that the citizen is likely to be in communication, or his means of communication are being used by the “person directly connected to the crime”, and also show why this communication is of essential importance to the investigation of the case. A judge must take into consideration this risk of arbitrariness as much as possible and critically assess the extent to which it is necessary to use covert investigative measures against other persons besides the alleged accused. Such a strict approach stems from the obligation stipulated by the Criminal Procedure Code itself, that the authorities carrying out covert investigative measure should limit, as much as possible, the communication and monitoring of persons who have no connection with the crime.¹⁰²

Covert investigative measures against a state-political official, a judge, or a person with immunity can be conducted only by the decision of a judge of the Supreme Court of Georgia, based on a substantiated motion by the Prosecutor General of Georgia or their deputy.¹⁰³ Maintaining a high standard for the protection of the right to private life for individuals involved in this activity is of particular importance for safeguarding political freedoms and fostering a healthy democratic environment in the country. Therefore, establishing a higher standard of protection on the legislative level is a commendable decision.

101 The general evidentiary standard for conducting investigative measures under the Criminal Code, which refers to a set of facts or information that would be sufficient for an impartial observer to conclude that a person may have committed a crime. Criminal Procedure Code, Article 3, Part 11.

102 Criminal Procedure Code, Article 143⁷ Part 1.

103 Ibid, Article 143³ Part 17.

Additionally, the use of covert investigative measures against clergy, doctors, journalists, and persons with immunity is permitted only if it does not involve obtaining information related to their professional activities.¹⁰⁴ In the case of a lawyer, any information obtained through covert investigation must be separated from the content of communication between the lawyer and the client, and any information related to the lawyer's professional activities must be destroyed immediately.¹⁰⁵ Thus, the obligation to destroy information related to professional activity is explicitly stipulated only for lawyers. However, such provisions are equally important for the activities of clergy, doctors, journalists, and persons with immunity. When conducting certain covert investigative measures in real time (e.g., telephone surveillance), there is an inherent risk that communications related to personal and professional activities may become intertwined, and information related to professional activities might "accidentally" fall within the scope of surveillance. Therefore, it is imperative that legislation adequately addresses this risk of improperly obtaining prohibited information.

2.6 The Procedure for Conducting Covert Investigative Measures and their Control Mechanisms

As already mentioned, the decision to conduct a covert investigation measure is made by a prosecutor, who submits a motivated motion to the district (city) court depending on the place of investigation.¹⁰⁶ A motivated motion must contain the circumstances that prove that:

- (1) investigation and/or criminal prosecution has been initiated for crimes defined by law;
- (2) there is a reasonable doubt to believe that a person against whom a covert investigative measure is to be carried out has committed any of the crimes ("a person directly connected with the crime"), or receives or transmits information that is intended for, or is provided by, the person directly connected with the crime, or the person directly connected with the crime uses the communication means of the person;

104 Ibid, Article 143⁷ Part 2.

105 Ibid, Article 143⁷ Part 3.

106 Criminal Procedure Code, Article 143³ Part 1.

- (3) covert investigative measures are carried out due to urgent public necessity and are a necessary, appropriate, and proportional means of achieving legitimate goals in a democratic society.
- (4) The information obtained as a result of covert investigative measures will be essential to the investigation and the obtaining of it is impossible or requires an unreasonable level of effort in any other way.¹⁰⁷

In addition to the listed criteria, it is desirable that the prosecutor's motion justifies why a particular covert investigative measure, in comparison to other investigative measures, is the most effective means of investigation. This justification is particularly important in cases where the prosecutor requests the use of multiple covert investigative measures simultaneously. Furthermore, since a covert investigative measure is conducted for a period specified in the judge's decision, and the law stipulates that the period must be as long as necessary to achieve the objectives of the investigation,¹⁰⁸ it is advisable for the prosecutor to provide a detailed justification for the duration and a tentative plan outlining how the requested covert investigative measure will be conducted. This plan should specify the investigative purposes and measures to be undertaken during the specified period.

A judge considers the prosecutor's motion within 24 hours of submission, in a closed court session, with or without an oral hearing, and makes a decision on conducting a covert investigative measure in the form of a decision.¹⁰⁹ Section 10 of Article 143³ lists the details that must be included in the judge's decision. In addition to verifying the technical aspects, a judge must critically analyze the arguments presented in the prosecutor's motion and assess the legality and necessity of conducting a covert investigative measure. Furthermore, it is desirable for a judge to provide a detailed justification in the decision, explaining why they did not deem it necessary to conduct covert investigative measures.¹¹⁰

The review of the motion is conducted in a closed session, and the decision is not announced publicly.¹¹¹ Consequently, the means of critically assessing judicial activity in the course of the case are very limited. This situation poses a risk that a

107 Ibid, Part 2, Subsections „a“-,„d“.

108 Criminal Procedure Code, Article 143³ Part 12.

109 Ibid, Part 5.

110 Criminal Procedure Code, Article 143³ Part 10.

111 Ibid, Part 13.

judge may adopt a superficial approach to the obligation to control the use of covert investigative measures or may excessively rely on the prosecutor's reasoning.

The Criminal Procedure Code provides for an exceptional rule for conducting covert investigative measures. In the case of urgent necessity, when the delay may lead to the destruction or loss of data important for the case, covert investigative measure can be started without a judge's decision, with the prosecutor's motivated resolution. Within 24 hours after the start of the covert investigative measure, the prosecutor must apply to the relevant court to acquire authorization for the covert investigative measure conducted as a matter of urgency. In the motion, the prosecutor must justify the urgent necessity and indicate the relevant factual circumstances.¹¹² A judge will review the motion within 24 hours of receiving it and make a decision to maintain or terminate the covert investigative measure used. In these proceedings it is becoming more evident to what extent courts trust the activities of the prosecutor and how critically it evaluates the prosecutor's decision.

A prosecutor makes the decision to terminate the covert investigative measure.¹¹³ The legislation provides for five grounds for terminating the covert investigative measures:

- (1) completion of the task stipulated by the decision on the covert investigative measure;
- (2) emergence of such circumstances that show that it is objectively impossible to perform the task provided for in the decision or that the use of covert investigative measure is no longer essential for the investigation;
- (3) termination of criminal prosecution and/or investigation;
- (4) Abolition of the basis in criminal law for carrying out covert investigative action;¹¹⁴
- (5) Expiration of the term determined by the court.¹¹⁵

In addition to the above, the covert investigative measure must be stopped immediately if it was started by the prosecutor without the authorization of the court on the grounds of urgent necessity and then the latter was recognized as illegal by the court.¹¹⁶

112 Ibid, Part 6.

113 Criminal Procedure Code, Article 143⁶ Part 1.

114 Ibid, Part 2.

115 Criminal Procedure Code, Article 143⁶ Part 3.

116 Ibid, Part 4.

The head of the personal data protection service holds the authority to suspend covert investigative measures conducted through the electronic control system if an electronic copy of the judge's motion or the prosecutor's resolution has not been received, or if there are discrepancies or ambiguities between the electronic and physical copies of the prosecutor's resolution.¹¹⁷ Upon rectification of these deficiencies, covert investigative measures can be continued.¹¹⁸

Thus, the grounds for suspension or termination of covert investigative measures are based on the approach that once a prosecutor is authorized to conduct covert investigative measures, courts no longer actively supervise the surveillance process. Consequently, the legislation does not provide for proactive judicial intervention in the use of covert investigative measures. This approach could be justified by the expectation that, ideally, a judge evaluates all necessary circumstances when issuing the authorization, ensuring that the decision does not require further verification. However, under this approach, judicial supervision is only reactive (depends on the prosecutor's motion) and applies solely at the authorization stage. For judicial supervision to be real and effective, courts must have the ability to engage in proactive, continuous monitoring of the covert investigative process. The legislation should thus include provisions allowing the court to independently verify the legality of the covert investigative measures or the relevance of the presented factual circumstances at the time of granting permission. In the event of identifying any deficiencies, the court should be empowered to halt the covert investigative measure and demand an explanation from the prosecutor.

As for the Personal Data Protection Service, courts are required to send a material copy of the decision to this agency no later than 48 hours after its issuance.¹¹⁹ In instances of covert monitoring and recording of telephone communications, the court decision containing only the requisites and the resolution part, is submitted to the Personal Data Protection Service by the operational-technical agency upon receipt, which commences the covert investigative measure once the receipt is confirmed.¹²⁰ In such cases, the head of the service has the authority to temporarily suspend the covert investigative measure if there are ambiguities or inaccuracies.

117 *Ibid*, Part 5.

118 *Ibid*, Part 13.

119 Criminal Procedure Code, Article 143³ Part 5.

120 Criminal Procedure Code, Article 143³ Part 51.

racies in the prosecutor's resolution, inconsistencies between the electronic and material requisites, or if the electronic copy has not been received.¹²¹

However, the inspector's authority is limited to halting the investigative measure conducted by the operational-technical agency through the electronic control system, and this power applies only to a single covert investigative measure.¹²² The Personal Data Protection Service is generally informed about the frequency of covert investigative measures and, in the case of covert monitoring and recording of telephone communications, can assist in clarifying the details of motions and decisions. However, the Service lacks the technical capability to monitor the actual implementation of other covert investigative measures, which raises concerns about its ability to fully exercise supervisory functions.

2.7 Stages and Terms for Implementation of Covert Investigative Measures

According to the legislation, the process of conducting covert investigative measures is divided into three stages. The first stage involves surveillance initiated on the basis of the court decision, with a duration not exceeding 90 days.¹²³ At the second stage, the surveillance measure can be extended for an additional period of no more than 90 days upon a motivated motion from the superior prosecutor to the court.¹²⁴ The third stage allows for a further extension of up to 90 days upon a judge's decision based on a motivated motion from the General Prosecutor or their deputy.¹²⁵ Therefore, the total duration of the covert investigative measure can last up to 270 days. If the intended objective cannot be achieved even after three extensions, the court may, based on a motivated motion from the Prosecutor General or their deputy, extend the term one more time for no more than 90 days, if the investigative measure is conducted under the law „On International Cooperation in the Field of Criminal Law“.¹²⁶ Additionally, if the crime falls under certain exceptions defined by the Code (e.g., intentional murder, illegal

121 Ibid, Part 5⁵.

122 Criminal Procedure Code, Article 143⁶ Part 5.

123 Criminal Procedure Code, Article 143³ Part 121.




124 Ibid

125 Ibid

126 Ibid, Part 12⁷, Subsection „a“.

imprisonment, trafficking, hostage-taking),¹²⁷ the period for conducting an covert investigative measure can be extended for a maximum of 90 days as many times as necessary to achieve the investigative objectives.¹²⁸

Table 1: Terms for Covert Investigative Measures

	Maximum Durations					In total
	I Stage	II Stage	III Stage	IV Stage	V Stage	
Most crimes	90 days	90 days	90 days			270 days
Cases stipulated by the Law "On International Cooperation in the Field of Criminal Law".	90 days	90 days	90 days	90 days		360 days
The exceptional crimes under the Criminal Procedure Code ¹²⁹	90 days	90 days	90 days	90 days	«As many times as» necessary	Statute of limitations for crimes ¹³⁰

It is important to emphasize that this arrangement resulted from the aforementioned and widely criticized legislative change of 2022. For contrast, it should be noted that prior to 2022, the Criminal Procedure Code set a maximum period of one month for covert investigative measures in the first stage. This term could be extended in the second stage for no more than two months. In the final, third stage, the extension was allowed for a period of no more than three months. The law did not provide for the possibility of a fourth extension of the term even in exceptional cases.¹³¹ Thus, before the 2022 changes, covert investigative measures could be conducted for a maximum of six months (180 days) in total. This term is markedly different from the new one established by the reform, which allows for up to nine months (270 days) for most cases, up to one year (360 days) in exceptional cases, and, for a rather large group of articles (more than 80, including up to

127 Ibid, Subsection „b“.

128 Criminal Procedure Code, Part 12⁷, Subsection „a“.

129 Articles 108, 109, 143, 143², 144-144³, 223-2241, 230-232, 234-2351, 2551, Article 260 Part 7, Article 261 Parts 4-8, Articles 262 and 263, Articles in these chapters: XXXVII-XXXVIII and XLVII.

130 Articles 108, 109, 143, 143², 144-144³, 223-2241, 230-232, 234-2351, 2551, Article 260 Part 7, Article 261 Parts 4-8, Articles 262 and 263, Articles in these chapters: XXXVII-XXXVIII and XLVII.

131 Criminal Procedure Code, Article 143³ as in 2020, 25th December version. Available at: <https://cutt.ly/cw3mufRe>. Updated: 28.03.2024.

10 punishable by less than one year of imprisonment), surveillance can continue indefinitely until the statute of limitations for the crime expires.

Table 2: Comparison of the Terms for the Use of Covert Investigative Measures

	Maximum Durations					In total
	Stage I	Stage II	Stage III	Stage IV	Stage V	
Until the 2021 reform	30 days	60 days	90 days			180 days
After the 2021 reform	90 days	90 days	90 days	90 days	"As many times as" necessary	270 days (1)
						360 days (2)
						Statute of limitations for crimes (3)

Each time an extension is requested, the representative of the prosecutor’s office is obliged to provide a motivated motion explaining why it was not possible to obtain sufficient data for the investigation during the previous period.¹³² Despite this provision, there remains an increased risk of disproportionate interference with human rights. Firstly, a judge may routinely extend an already initiated covert investigative measure without critically evaluating the prosecution’s explanation for the inability to achieve the required objectives within the specified time frame. Additionally, the flexible nature of surveillance extensions encourages courts and investigative bodies to view covert investigative measures not as exceptional, last resort measures, but as standard, routine methods for obtaining evidence.

In the 2023 report of the Personal Data Protection Service, it is indicated that the common courts considered 228 motions regarding the extension of the period of covert monitoring and recording of telephone communications, of which 220 were fully or partially granted (198 fully, 22 partially), resulting in a rather high authorization rate of 96.5%.¹³³ A similar trend was observed in 2022: the courts considered 288 motions regarding the extension of the period of covert monitor-

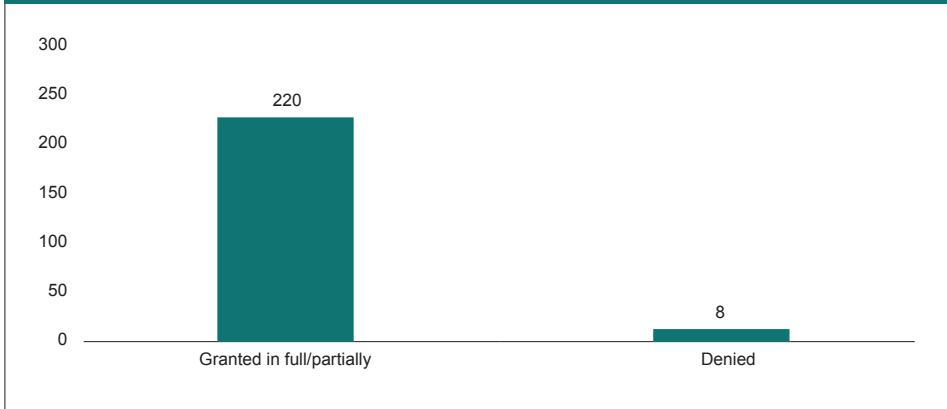
¹³² Criminal Procedure Code, Article 143³ Part 12⁸.

¹³³ Personal Data Protection Service (2023). “Activity Report,” 142. Available at: <https://cutt.ly/1eishkc>. Updated: 02.04.2024.

ing and recording of telephone communications, of which 265 were fully or partially granted (204 fully, 61 partially), yielding an authorization rate of 92%.¹³⁴ In 2023, the courts considered 122 motions regarding the extension of the period of covert video and/or audio recording and photographing, of which 115 were fully or partially granted (113 fully, 2 partially).¹³⁵ In 2022, the courts considered 186 such motions, of which 144 were fully or partially granted (144 fully).¹³⁶

Furthermore, the extended duration does not push investigative bodies to conduct timely and effective investigations or to reevaluate their investigative strategies. Based on similar reasoning, the Venice Commission, in its evaluation of the 2022 legal reform, also noted that the possibility of multiple extensions of surveillance periods, especially “as many times” as necessary in the case of certain crimes, constitutes excessive interference with human rights.¹³⁷

Figure 2: Statistics on the Term Extensions for Wiretapping and Recording of Telephone Communications (2023)



134 Ibid

135 Ibid, 144.

136 Ibid

137 Georgia - Urgent opinion on the Draft Law on the Amendments to the Criminal Procedure Code adopted by the Parliament of Georgia on 7 June 2022, 11.

Figure 3: Statistics on the Term Extensions for Wiretapping and Recording of Telephone Communications (2022)

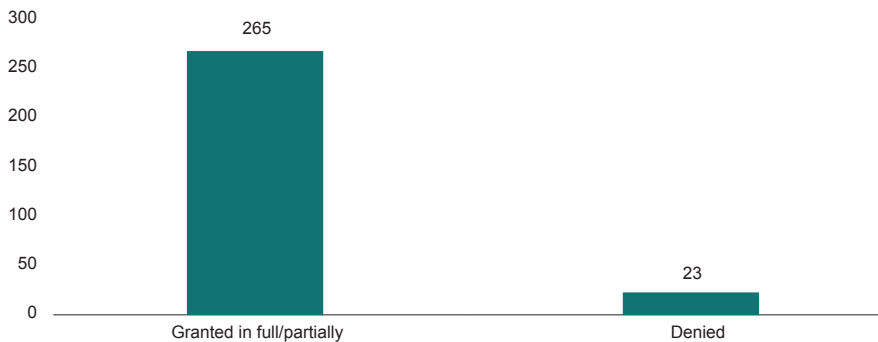


Figure 4: Statistics on the Term Extensions for Covert Video and/or Audio Recording, Photographing (2023)

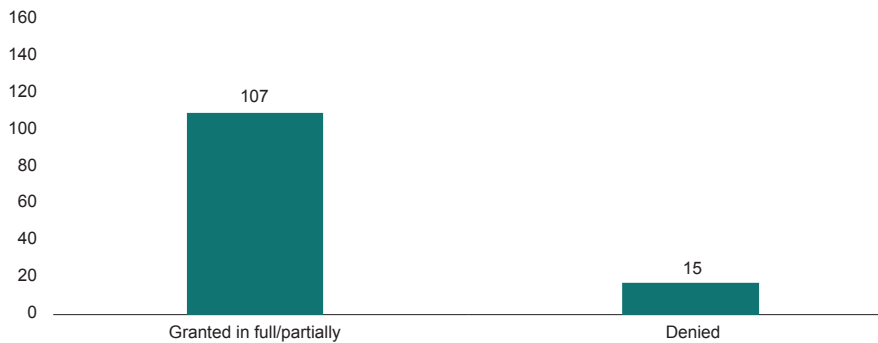
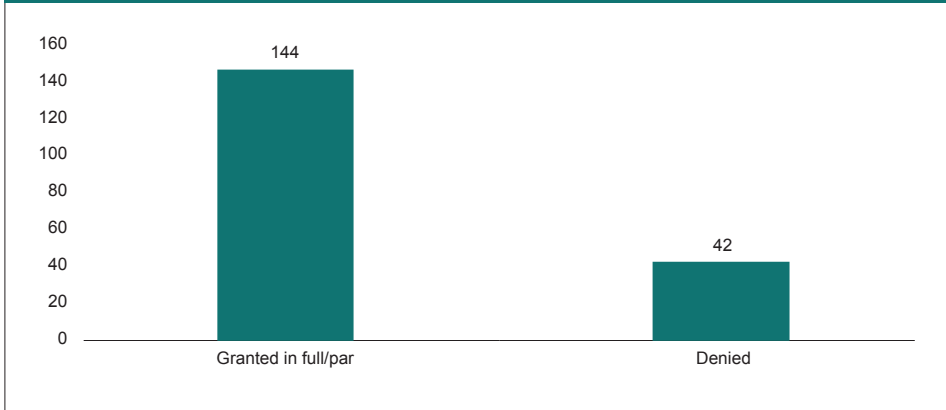


Figure 5: Statistics on the Term Extensions for Covert Video and/or Audio Recording, Photographing (2022)



2.8 Notification on Covert Investigative Measures and Appeals Mechanisms

The Criminal Procedure Code provides two mechanisms for a citizen to challenge the legality of a covert investigative measure. The first mechanism applies when an individual becomes aware of a covert investigative measure against them during the proceedings of their case. In this case, an individual may appeal the decision on the covert investigative measure to the Investigative Panel of the Court of Appeal once.¹³⁸ This appeal must be filed within 48 hours of receiving the notification about the surveillance and an explanation of the right to appeal the decision.¹³⁹ In instances where an individual becomes aware of the covert investigative measure after the conclusion of the case proceedings, the appeal period extends to one month.¹⁴⁰ If the appellate court deems the investigative measure illegal, the evidence obtained through such means may be considered inadmissible.¹⁴¹ In cases that have already been completed, this finding can serve as a basis for revising the decision.¹⁴² Furthermore, based on the decision regarding the complaint, the individual may seek compensation for damages resulting from the illegal acquisition, storage, or disclosure of personal information or personal data.¹⁴³

138 Criminal Procedure Code, article 143³, part 14.

139 Ibid

140 Ibid, part 15.

141 Ibid

142 Ibid

143 Criminal Procedure Code, article 7, part 3.

It should be noted that the 48-hour period is rather brief for a citizen to adequately prepare a legal complaint. Additionally, there is ambiguity regarding what constitutes “becoming aware” of the surveillance, how a citizen is expected to prove receipt of the notification, what is the burden of proof in a given case, and the precise point at which the appeal deadline should be calculated. Procedural legislation should ensure accessible justice for citizens potentially affected by surveillance and provide effective avenues for the restoration of potentially violated rights. However, strict deadlines and vague language complicate this process, potentially discouraging citizens from exercising their rights.

Regarding the second mechanism of appeal, it is based on the investigative bodies’ obligation to notify the individual in writing about the covert investigative measure conducted against them after its completion or termination. This notification must include the judge’s decision, accompanying materials, and information about the right to appeal.¹⁴⁴ The prosecutor determines the precise timing of when this notification should be sent.¹⁴⁵ If the prosecutor decides not to send the notification within 12 months after the conclusion of the covert investigation, they are required to apply with the motion to the judge who made the initial decision no later than 72 hours before the expiration of this period, seeking to postpone the notification for no more than an additional 12 months.¹⁴⁶ In this motion, a prosecutor must justify the potential threat the notification poses to the interests of the investigation and proceedings.¹⁴⁷ A prosecutor may similarly postpone the notification for two more 12-month periods.¹⁴⁸ Consequently, the notification to an individual regarding a covert investigative measure can be postponed for a maximum of 48 months. For comparison, according to the legal regulation of the procedure in the 2021 version, the individual had to be informed about the covert investigative measures within 12 months of their conduct. This period could be extended twice by 12 months each, allowing a maximum postponement of 36 months. In relation to specific crimes (the same crimes for which the duration of covert investigative measures can be extended indefinitely), the notification may be postponed “as many times as necessary” to protect the interests of state security, public order, and legal proceedings.¹⁴⁹

144 Criminal Procedure Code, article 143⁹, part 4.

145 Ibid, part 3.

146 Ibid, part 4.

147 Ibid, article 143⁹, part 4.

148 Ibid, part 5.

149 Ibid, part 4.

While there may be an objective need to postpone notification, and theoretically, a judge can critically evaluate such requests, the potential for lengthy postponements¹⁵⁰ poses a significant risk of prolonged and intense interference with human rights. In turn, this situation creates favorable conditions for the abuse of power and arbitrariness by investigative bodies. Additionally, the longer the delay in notifying the citizen about the surveillance, the less likely they are to be interested in or motivated to appeal, as their legal and factual interest in the incident diminishes over time. Furthermore, since the final decision on notification is made by a prosecutor, a judge does not oversee compliance with notification deadlines.¹⁵¹ Consequently, the risks of abuse of this authority are particularly high and are not effectively supervised.

It should be noted that the existing notification mechanism has been criticized in the 2023 report of the Public Defender. The report highlights that the notification procedure lacks clarity. Specifically, it is unclear whether a citizen should receive a written notification or it suffices that he/she obtains the information in person at the prosecutor's office; whether citizens can familiarize themselves with the content of the information collected about them, or notification about the conduct of covert investigative measures is sufficient; whether citizens can learn about the materials subject to destruction or only the fact of their destruction is notified.¹⁵² The report also mentions that the Prosecutor General issued Order #211-c on November 4, 2022, directing prosecutors to provide written notification to individuals about the conduct of covert investigative measures, the content of the material obtained, and the destruction of such material. However, this order is not publicly available, and the Prosecutor General has refused to provide it to the Public Defender's Office, citing that the document is intended solely for internal use.¹⁵³

The notification mechanism, beyond enabling parties to access evidence in criminal proceedings, is effectively the sole means by which investigative bodies are required to disclose surveillance information to citizens. Additionally, it serves as a critical tool for the public to assess the effectiveness of judicial oversight, since unlike the decision

150 Ibid, part 7.

151 This claim was also confirmed by the Tbilisi City Court in response to a letter responding to the request for public information by the Social Justice Center.

152 Public Defender of Georgia (2023), "Report on the State of Protection of Human Rights and Freedoms in Georgia," 143. Available at: <https://cutt.ly/2eis1RDo>. Updated: 02.04.2024.

153 Ibid

to conduct a covert investigative measure, the decision on a complaint is made public and, upon request, is provided to the complainant and the prosecution.¹⁵⁴ Consequently, this mechanism is the principal lever for demanding public oversight of surveillance cases and legal responses to violations of individual rights. However, the effectiveness of this mechanism is severely limited by legislative provisions permitting the delay of notification. In its assessment of the 2022 legislative changes, the Venice Commission also criticized the extension of the notification period, emphasizing the risk that absence of notification or unreasonably late notification could become a routine practice rather than an exception.¹⁵⁵

2.9 Familiarization with, Storage and Destruction of Information Obtained as a Result of Covert Investigative Measures

Only a prosecutor, judge, and investigator have the right to access the information obtained through covert investigative measures until the completion of this measure.¹⁵⁶ The defense is also notified of the information no later than five days before the pre-trial session and at the time of signing the plea agreement.¹⁵⁷ If the material obtained from a covert investigative measure holds no value for the investigation, it must be destroyed immediately following the termination or completion of the measure, as per the prosecutor's decision.¹⁵⁸ Additionally, if the information obtained under urgent necessity, irrespective of its legal recognition by the court, is not submitted by the prosecution as evidence during the merits consideration, it must be destroyed immediately.¹⁵⁹ The responsibility for destroying this material lies with the prosecutor supervising the investigation, prosecutor presenting the state claim, or their superior prosecutor, in the presence of the judge who authorized or legalized the covert investigative measure. This authority can also be exercised by another judge of the same court.¹⁶⁰

154 Criminal Procedure Code, article 143³, part 16.

155 Georgia - Urgent opinion on the Draft Law on the Amendments to the Criminal Procedure Code adopted by the Parliament of Georgia on 7 June 2022, 12.

156 Criminal Procedure Code, article 143⁹, part 1.

157 Ibid, part 2.

158 Criminal Procedure Code, article 143⁸, part 1.

159 Ibid

160 Ibid, part 5.

As for the material that the court recognizes as inadmissible evidence or that is attached to the case as material evidence, the obligation to retain it rests with the court. After a specified period, this material is destroyed by the judge who authorized the covert investigative measure or by another judge of the same court.¹⁶¹

In the process of carrying out a covert investigative measure, the operational-technical agency has the right to copy information, creating the technical possibility and potential motivation for establishing an illegal “alternative bank of files”¹⁶². This concern is particularly relevant given that the agency falls under the governance of the Security Council, which, as a body with investigative and counter-intelligence functions, has a professional interest in acquiring as much information as possible.¹⁶³ Although the Personal Data Protection Service has the authority to check the legality of data processing through electronic control of activities conducted in the central data bank, including entering the restricted access area of the agency, monitoring ongoing activities, requesting explanations, and exercising other powers,¹⁶⁴ alternative data banks can still remain secret. This is due to the fact that the service can only enter the agency’s territory within the “restricted access area”¹⁶⁵. Given this limitation, the legislation should incorporate more effective mechanisms for the meaningful oversight of the operational-technical agency’s activities.

The Constitutional Court’s decision of April 14, 2016, was based on this logic, noting that the possibility for a state agency to control both investigative functions and technical means of surveillance simultaneously increased the risks of arbitrary and excessive interference in human rights: “Risks of human rights’ infringements are inherently heightened when the SSSG (or any other body with investigative powers) simultaneously owns and administers the technical means.”¹⁶⁶

The risks associated with the institutional structure of the SSSG are exacerbated when oversight mechanisms are insufficiently effective. Concerning the authority

161 Ibid, part 6.

162 Decision of the first panel of the Constitutional Court of Georgia No. 1/1/625,640. April 14, 2016, Para. 100.

163 Ibid para. 55.

164 Law of Georgia “On Personal Data Protection”, article 40¹⁶, part 7.

165 Ibid, „a“ subsection.

166 Decision of the first panel of the Constitutional Court of Georgia No. 1/1/625,640. April 14, 2016, Para. 53.

of surveillance by the State Security Service, the Constitutional Court observes that “the existing levers of the inspector’s control over the covert wiretapping are inadequate; they cannot eliminate the risk of circumvention of inspector’s control and, consequently, the risk of monitoring telephone conversations without judicial authorization”.¹⁶⁷ During the deliberation of the case, expert testimony corroborated the technical feasibility for the SSSG to establish a so-called parallel infrastructure, which would not be subject to the control of the Personal Data Protection Service. Ultimately, the court concluded that the contested provisions “enable the state security service, through modern technologies, to acquire personal information about an indeterminate group of individuals. Although there is a presumption that an authority vested with the appropriate power will not misuse these technical means, the creation, possession, and administration of technical capabilities (including software) to obtain personal information in real-time, and the potential for direct access to personal information using these means, along with the capability of copying and storing personally identifiable data (metadata) by an agency tasked with investigative functions or possessing a professional interest in this information, significantly heightens the risk of unwarranted intrusion into private life”.¹⁶⁸

Precisely based on the aforementioned decision was the operational-technical agency established. At first glance, this agency appears to only technically implement covert investigative measures and has no investigative functions. However, its real institutional independence is still questionable, as it is an LEPL within the State Security Service. Consequently, the legislative changes did not effectively fulfill the objectives of the Constitutional Court’s 2016 decision, as the agency is not an independent entity separate from the State Security Service. This criticism formed the basis for a significant segment of civil society when, in 2017, they filed another lawsuit with the Constitutional Court, demanding an evaluation of the extent to which the legislative reforms of 2017 adhered to the court’s decision of April 14, 2016.¹⁶⁹

167 Decision of the first panel of the Constitutional Court of Georgia No. 1/1/625,640. April 14, 2016, Para. 59.

168 Ibid, Para. 117.

169 Freedom of Information Development Institute (2017). “Regulation of surreptitious surveillance in Georgia (January-August, 2017)”, 5. Available at: <https://cutt.ly/Sw3mXRxN>. Updated: 28.03.2024.

2.10 Transparency of Judicial Oversight over the Use of Covert Investigative Measures

For high public trust and accountability in the security sector, it is imperative that information about the activities of supervisory bodies is accessible to the public. Regarding the transparency of judicial oversight of covert investigative measures, the Criminal Procedure Code provides a singular mechanism: a registry of covert investigative measures maintained by the Supreme Court.¹⁷⁰ This registry includes statistical information pertinent to covert investigative measures. Specifically, it documents information on motions submitted to the courts and the subsequent decisions made by the courts concerning the authorization of covert investigative measures. Additionally, it contains information on the destruction of materials obtained from operational-search measures that were unrelated to an individual's criminal activity but contained personal information about them or others. Consequently, the law mandates that the Supreme Court collects and publishes statistical data on these motions and court decisions.

Since the law does not explicitly detail the specific types of data to be processed or the required level of accuracy, the Supreme Court must determine the methodology for data collection, visualization, and analysis. An analysis of the statistical data published by the Supreme Court from 2014 to 2022 indicates the existence of a relatively consistent methodological approach. However, it is important to note that the documents outlining this methodology are not publicly accessible.

According to the established practice, the court annually publishes statistical data processed in Excel documents, which provide the following information: the total number of motions filed in district and city courts, categorized as granted, partially granted, not granted, or inadmissible.¹⁷¹ Additionally, the statistical data include the total number of cases involving the destruction of materials obtained through operational search measures. These materials refer to information unrelated to an individual's criminal activities but containing personal information about them or others. Moreover, the court publishes the total number of instances of one specific covert investigative measure – namely, the covert wiretapping and recording of telephone communications – broken down by city and district court and by the qualification of the crime.

¹⁷⁰ Criminal Procedure Code, article 143¹⁰, part 1.

¹⁷¹ Supreme Court of Georgia (2022). Basic statistical data of common courts. Available: <https://cutt.ly/vw3mV35H>, Updated: 28.03.2024.

It is important to note that the statistical data published by the court are so limited and fragmented that they do not allow for the drawing of either analytical or descriptive conclusions regarding the use of covert investigative measures. For instance, although the court has the capability, it does not publish statistics on the following indicators:

- Total number of persons against whom covert investigative measures were used;¹⁷²
- Number of specific covert investigative measures categorized according to district/city courts and crime qualification (at this stage, the court processes this data only in case of covert monitoring and recording of telephone communication);¹⁷³
- If more than one covert investigative measure is used, the frequency of measures used at the same time (this information would allow us to assess which covert investigative measures have complementary functions in the investigation process, whether they overlap with each other, etc.);
- The frequency and average duration of extension of covert investigative measures;¹⁷⁴

172 According to the information provided by the Personal Data Protection Service, from March 1, 2022 to December 31, 2022, covert surveillance and recording began against 2,852 persons, and from January 1, 2023 to December 31, 2023 - against 2,506 persons. As the 2022 data on persons is partial, it is not possible to compare it with the annual number of rulings. And in the case of 2023, as the data published by the Supreme Court shows, the covert wiretapping and recording of telephone communication was granted with 744 decisions. Accordingly, with one decision, the hearing was started against an average of 3 persons.

173 It was possible to obtain fragmented information on a specific covert investigative action, in particular, covert video and audio recording, based on an application to the Personal Data Protection Service. In particular, in 2023, the service informed the Social Justice Center that in 2021, the general courts heard 406 petitions related to covert video and audio recording, of which 399 were granted. In 2022, 614 petitions regarding the use of the same action were submitted to the courts, of which 583 petitions were granted. It should be noted that the service refused to share the same information in 2024, noting that the service, which was established on March 1, 2022, did not have access to the materials of previous years. In addition, the service indicated that it had the opportunity to produce statistics only in the case of covert monitoring and recording of telephone communications.

174 According to the information provided by the Personal Data Protection Service, from March 1, 2022 to December 31, 2022, 881 rulings were heard for up to 30 days, 64 rulings - for up to 60 days, and 178 rulings - for up to 90 days. The average duration of these actions was 29 days. As for 2023, in 365 decisions, orders were issued for up to 30 days, in 96 decisions - for up to 60 days, and in 521 decisions - for up to 90 days. In total, the average duration of actions in 2023 was 50 days.

- The frequency of appeals of covert investigative measures by citizens;¹⁷⁵
- The number of covert investigative measures conducted against state-political officials, judges and persons with immunity;¹⁷⁶
- The number of persons who were informed about the conduct of a covert investigation;¹⁷⁷
- The number of persons notified of the destruction of the material obtained as a result of covert investigative measures;
- Frequency of postponing the notification to the relevant person about the conduct of covert investigative measures, etc.

Although the obligation to produce statistics on these indicators is not explicitly stated in the general legislative provisions, the Supreme Court, if acting in good faith and in the public interest, has the capability to process statistical data on the aforementioned indicators. This is particularly pertinent given that information on these indicators is already available in a fragmented manner through other agencies. Therefore, the Supreme Court could voluntarily assume the responsibility to collect and publish this information.

According to Section 17 of Article 143³ of the Civil Code, a covert investigative measure against a state-political official, judge, or person with immunity may be carried out only by the decision of a judge of the Supreme Court of Georgia, based on a motivated motion from the Prosecutor General of Georgia or their deputy. The statistics published in the Registry of Covert Investigations include only motions filed in city courts and the decisions issued on

175 Although, according to the law, a citizen can appeal an covert investigative action in the appeals court, the Tbilisi appeals court informed us that it does not record statistical data regarding the number of appeals.

176 In 2024, the General Prosecutor's Office of Georgia informed the Social Justice Center that in 2017-2023, the Prosecutor General applied to the Supreme Court with a total of 10 petitions. The Prosecutor's Office refrained from announcing the decision of the court regarding the mentioned motions and urged us to contact the Supreme Court. In response to the letter of March 7, 2024, the Personal Data Protection Service informed us that in the period 01.03.2022 - 31.12.2023, the Personal Data Protection Service did not receive such rulings from the court. In turn, the Supreme Court refused to share this information with the argument that maintaining a registry of covert investigative activities did not include the obligation to process this data (more below).

177 In response to a letter requesting public information from the Social Justice Center, the Prosecutor General of Georgia informed us that in 2023, 1,352 persons were notified in writing about the conduct of an covert investigation. The Supreme Court informed us that since the decision on the notification is made by the prosecutor, therefore the Supreme Court does not have information about compliance with the notification deadlines. The same information was confirmed by the Tbilisi City Court.

them, but do not record the motions filed with the Supreme Court. The Social Justice Center requested this information from the Supreme Court as public information. However, the court responded that this data is not recorded in the registry.¹⁷⁸ In response, the Social Justice Center filed an administrative complaint with the Supreme Court, demanding that the authorized person of the Supreme Court be instructed to process statistical information about the motions submitted to the Supreme Court from 2016 to 2022. During the oral hearing, the Social Justice Center argued that the requested information is available to the Supreme Court in the form of raw data, constitutes public information, and hence, the court is obliged to process this data statistically and amend the methodology for producing the registry of covert investigative measures in the future. The representative of the Supreme Court did not agree with this request and reiterated that the information is not recorded in the Supreme Court's statistics. Ultimately, the Supreme Court refused to satisfy the administrative complaint. The Social Justice Center did not accept this reasoning and subsequently filed a lawsuit against the Tbilisi City Court and the Supreme Court, seeking a decision to compel the Supreme Court to process and share the data from 2016 to 2022 with the Center and to make changes to the methodology of the statistical registry when processing future statistical data.

Comprehensive statistics on covert investigations should include information on motions filed in both city (district) courts and the Supreme Court. The wording of Article 143¹⁰ clearly indicates that the legislator intended for such statistics to be produced, as it uses the term "courts," which refers to both the city courts and the Supreme Court, without specifying that the obligation to produce statistics applies only to motions filed in city courts. It does indicate that the Supreme Court is exempt from this rule. The purpose of maintaining the registry is to ensure transparency and accountability of judicial and investigative services, and to properly inform the public about the frequency and extent of covert investigative measures. Therefore, incomplete data collection, especially when covert investigative measures are carried out against individuals with special status (state-political officials, judges, and persons with immunity), fundamentally undermines the primary objectives of producing these statistics.

178 The response of the Supreme Court of Georgia dated 03.10.2023 to the letter of the Social Justice Center.

To ensure the country's democratic development and political freedom, it is essential that the legislation provides special guarantees to protect judges, politicians, high-ranking officials, and representatives of the diplomatic corps from illegal surveillance. This is the primary purpose of Section 143¹⁰, according to which only the Prosecutor General (or their deputy) is authorized to file a motion, and only the Supreme Court has the power to issue a warrant for surveillance. Public interest in the publication of statistical data on these cases is particularly high, as it should inform the public about the frequency with which politically significant individuals become targets of surveillance and the effectiveness of the court's oversight in this process. Consequently, the Supreme Court is obligated to proactively process this information and publish it annually, in line with the transparency objectives of judicial oversight.

It is important to note that the Supreme Court does not engage in the analytical and narrative processing of descriptive statistical data. For instance, the Court does not identify or analyze the trends and established practices related to the use of covert investigative measures, publish annual reports or discuss the substantive elements of judicial oversight. Given that court decisions on motions are not announced in public, and the copies of court decisions are withheld by the court on grounds of their classified nature,¹⁷⁹ the Supreme Court needs to proactively process the arguments presented in the court decisions and motions and publish reports on their general content and core tendencies.

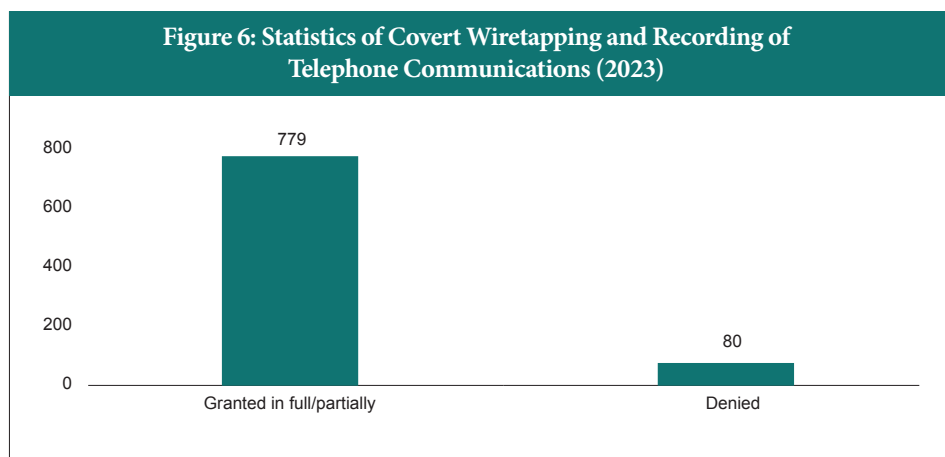
Consequently, the public is inadequately informed about the effectiveness of the oversight on covert investigative measures, and the court fails to meet the standards of transparency and accountability. In this regard, the court should adopt a more transparent approach and proactively provide information to the public. Such a strategy would illustrate to what extent the court's oversight over covert investigative measures is effective and whether it applies a standard that justifies interference with human rights when granting permission.

¹⁷⁹ Tbilisi City Court's 28.03.2023 response to the letter of the Social Justice Center.

2.11 Trends Identified in Statistical Data

This chapter analyzes the trends identified in the statistical data published in the Supreme Court's registry of covert investigative measures.

It is important to note that in 2023,¹⁸⁰ the Supreme Court published statistical data solely concerning the covert wiretapping and recording of telephone communications.¹⁸¹ Due to the lack of comprehensive statistical indicators, it remains impossible to ascertain the total number of motions filed in common courts, the number of motions granted, or the proportion of wiretapping and recording of telephone communications within the overall total. The available data indicates that in 2023, 859 motions were filed in common courts concerning the covert wiretapping and recording of telephone communications. Out of these, 779 were either fully or partially granted (744 fully and 35 partially), representing 90.68% of the total.



In 2023, as in previous years, wiretapping and recording of telephone communications were most frequently associated with membership of the 'criminal underworld' and 'being a thief in law'.

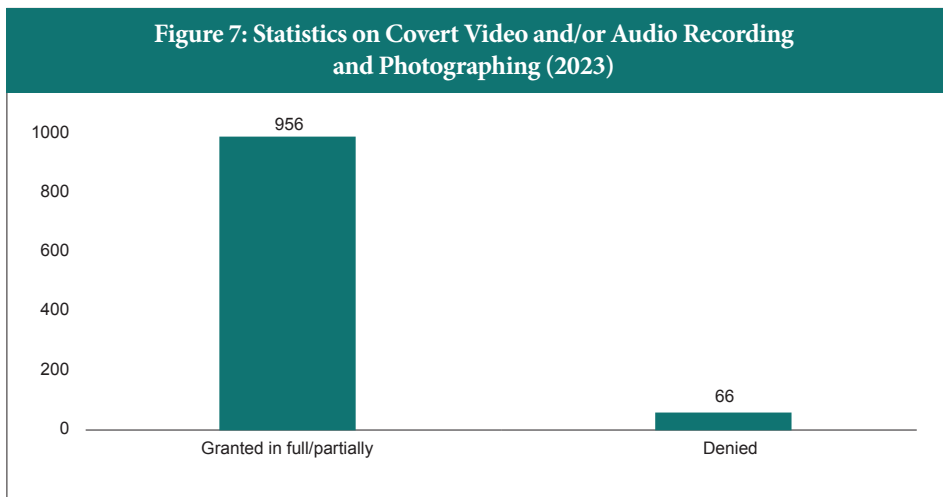
¹⁸⁰ As of 01.04.2024.

¹⁸¹ Supreme Court of Georgia (2023). Basic statistical data of common courts. Available: <https://www.supremecourt.ge/ka/news>. Updated: 28.03.2024.

Table 3: Top Ten Most Prosecuted Crimes (2023)

Definition	Judicial Review	Granted in full/partially
Membership of the ‘criminal underworld’; ‘being a thief in law’ (Article 223 ¹)	197	189
Fraud (Article 180)	106	100
Illegal manufacturing, production, purchase, storage, transportation, transfer or sale of drugs, their analogues, precursors or new psychoactive substances (Article 260)	69	61
Taking bribes (Article 338)	40	40
Intentional infliction of serious harm to health (Article 117)	37	25
Intentional murder (Article 108)	34	23
Extortion (Article 181)	33	33
Legalization of illegal income (money laundering) (Article 194)	29	27
Misappropriation or embezzlement (Article 182)	27	25
Intentional murder under aggravating circumstances (Article 109)	18	16

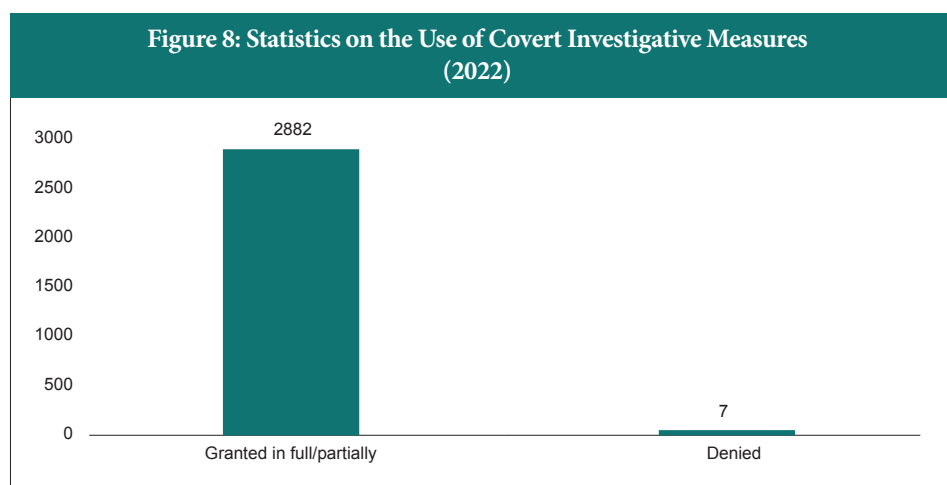
The Personal Data Protection Service’s 2023 report additionally provides statistical data on covert video and/or audio recording, photographing. In particular, according to the service, in 2023, the common courts considered 1022 motions, of which 956 were fully or partially granted (952 - fully, 4 - partially) constituting 93.5%.¹⁸²



¹⁸² Personal Data Protection Service (2023). “Activity Report”, 143. Available at: <https://cutt.ly/1eisskcc>. Updated: 02.04.2024.

The report of the Personal Data Protection Service also mentions that in 2023, the common courts considered a total of 3 motions regarding the removal and fixation of information from communication channels, computer systems, out of which 1 was granted, 2 – was not.¹⁸³

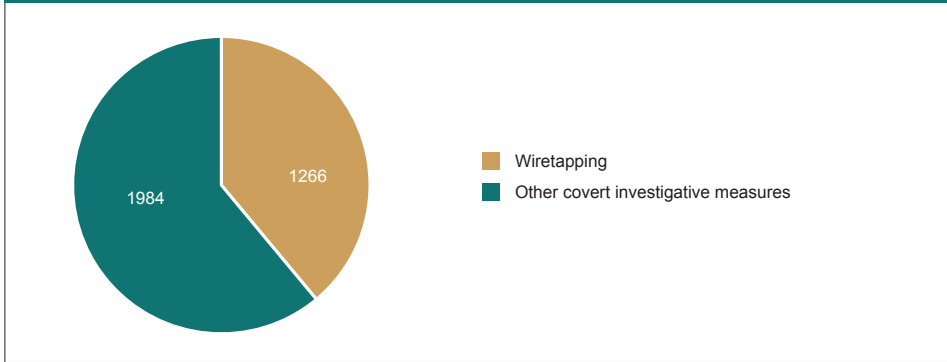
Statistical information published by the Supreme Court shows that in 2022, a total of 3,250 motions were filed in common/city courts, of which 2,685 were fully and 197 partially granted (in sum 2,882). Accordingly, the percentage of the granted motions is 88.7%, which shows that the rate of granting motions was rather high in 2022.



In addition to the overall number of covert investigations, the Supreme Court Registry also publishes separate statistics on covert wiretapping and the recording of telephone communications. According to these statistics, in 2022, 1,266 motions were submitted to the court for the covert wiretapping and recording of telephone communications, amounting to 47.1% of the total number of covert investigative measures. This data suggests that the Prosecutor’s Office employs this type of covert investigative measure as its primary surveillance mechanism.

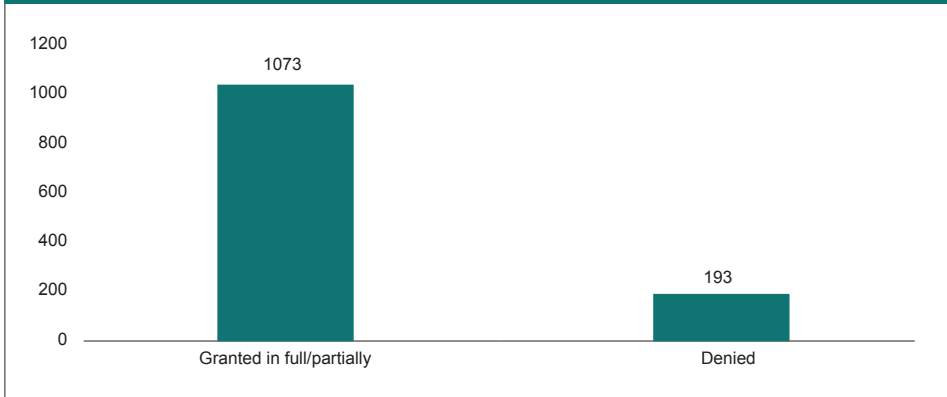
183 Personal Data Protection Service (2023). “Activity Report”, 150. Available at: <https://cutt.ly/1eishkc>. Updated: 02.04.2024.

Figure 9: Frequency of Wiretapping Versus Frequency of other Covert Investigative Measure (2022)



The analysis of statistical data shows that the rate of granting the motions regarding the covert wiretapping and recording of telephone communication is 84.7%.

Figure 10: Wiretapping Statistics (2022)



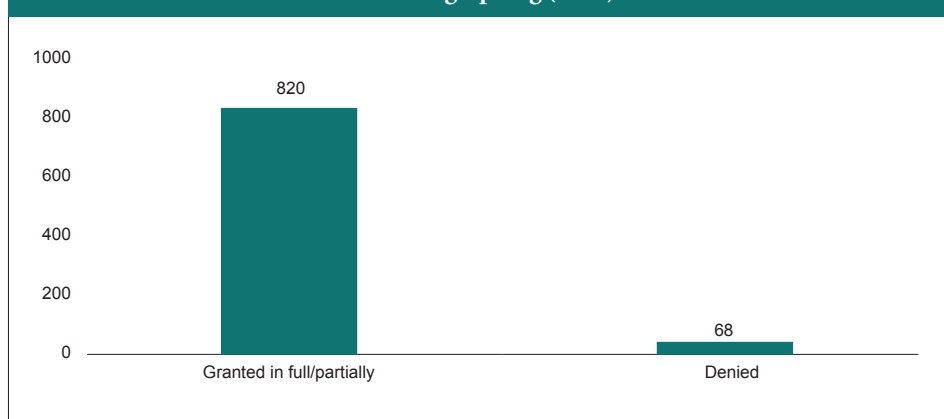
As known, the registry publishes detailed statistics on the use of covert investigative measures under the articles of the Criminal Code only in relation to the covert wiretapping and recording of telephone communications. According to the given statistics, it turns out that in 2022 wiretapping was most frequently used in cases related to the membership of the ‘criminal underworld’.

Table 4: Top Ten Most Prosecuted Crimes (2022)

Definition	Judicial Review	Granted in full/partially
Membership of the ‘criminal underworld’; ‘being a thief in law’ (Article 223 ¹)	291	255
Fraud (Article 180)	140	122
Theft (Article 177)	100	56
Illegal manufacturing, production, purchase, storage, transportation, transfer or sale of drugs, their analogues, precursors or new psychoactive substances (Article 260)	91	81
Intentional murder (Article 108)	68	60
Intentional infliction of serious harm to health (Article 117)	55	34
Extortion (Article 181)	46	39
Legalization of illegal income (money laundering) (Article 194)	38	38
Taking bribes (Article 338)	33	31
Manufacturing, sale or use of forged credit or debit card (Article 210)	32	30

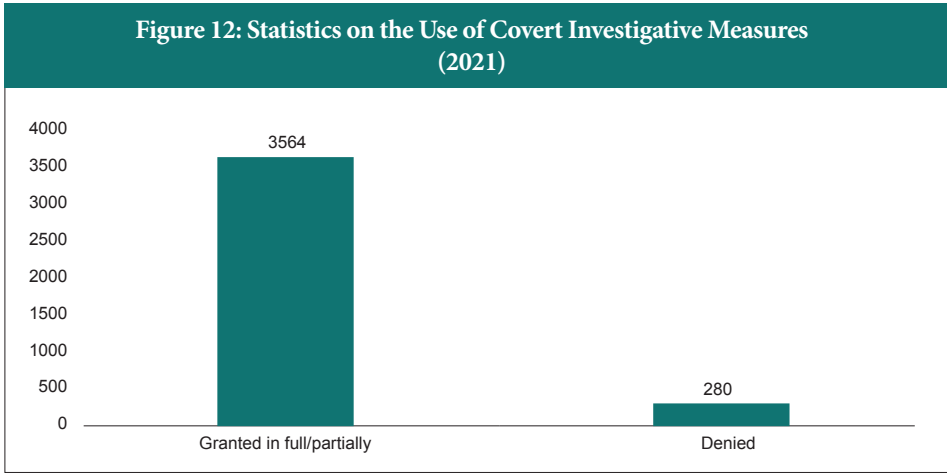
In the 2023 report of the Personal Data Protection Service, separate statistics on covert video recording and/or audio recording, photographing are indicated. According to the service, in 2022, courts considered a total of 888 motions, of which 820 were fully or partially granted (811 - fully, 4 - partially) constituting 92.34%.¹⁸⁴

Figure 11: Statistics on Covert Video and/or Audio Recording and Photographing (2022)

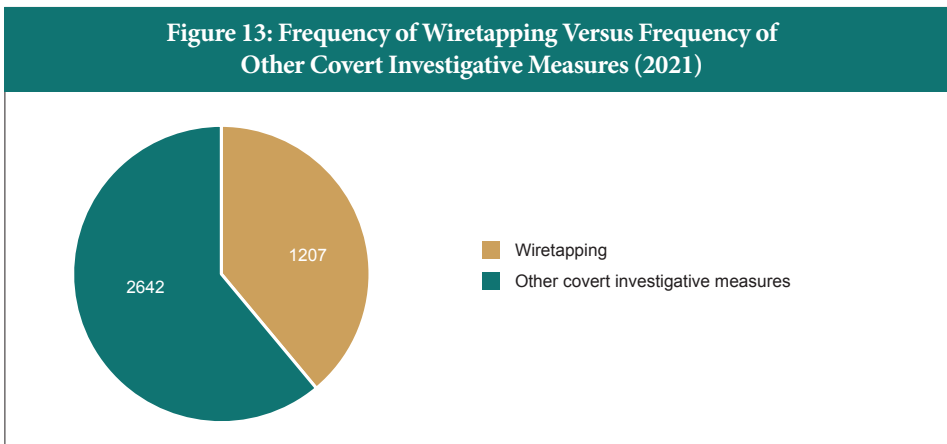


¹⁸⁴ Personal Data Protection Service (2023). “Activity Report”, 150. Available at: <https://cutt.ly/1eishkc>. Updated: 02.04.2024.

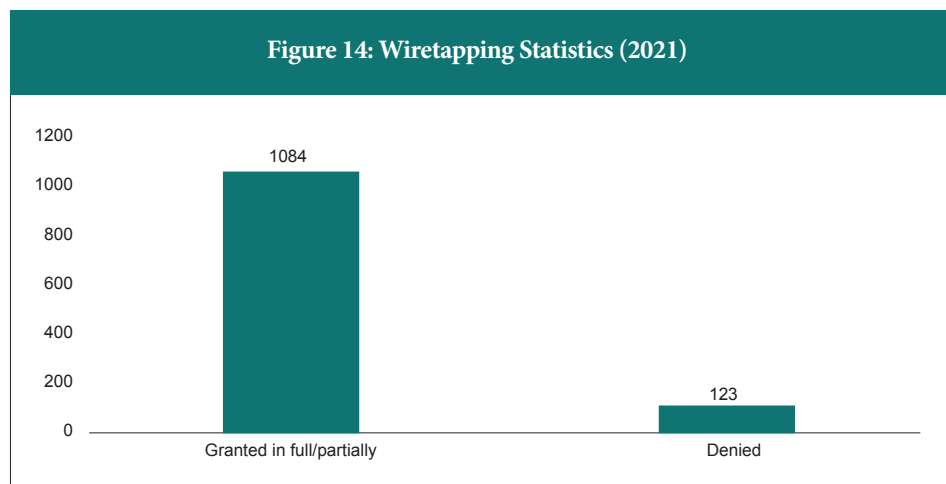
The analysis of statistical data of 2021 shows that a total of 3,849 motions regarding the use of covert investigative measures were submitted to the courts, of which 3,564 were fully or partially (3,497 - fully, 67 - partially) granted constituting 92.6%. This shows that in 2021, the authorization rate of covert investigative measures was even higher than in 2022.



In 2021, a total of 1,207 motions were submitted to the court for authorization of covert wiretapping and recording of telephone communications, which is 31.4% of the total number of covert investigative measures. Since the Supreme Court does not publish detailed statistics on the use of other covert investigative measures, it is not possible to compare the frequency of wiretapping and recording with other types of covert investigative measures.



The statistics on wiretapping show that 1084 out of 1207 motions were fully or partially granted constituting 89.8%.

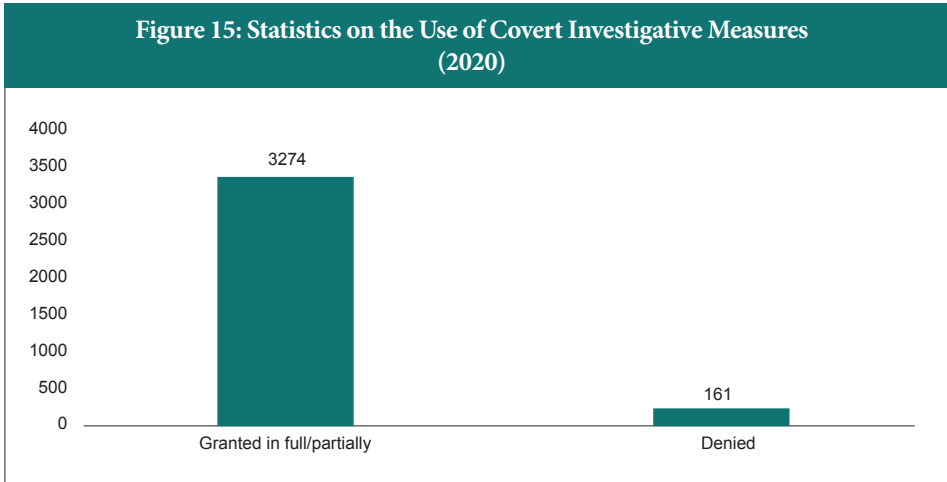


Statistics show that even in 2021, wiretapping was most often conducted in cases related to membership of the ‘criminal underworld’.

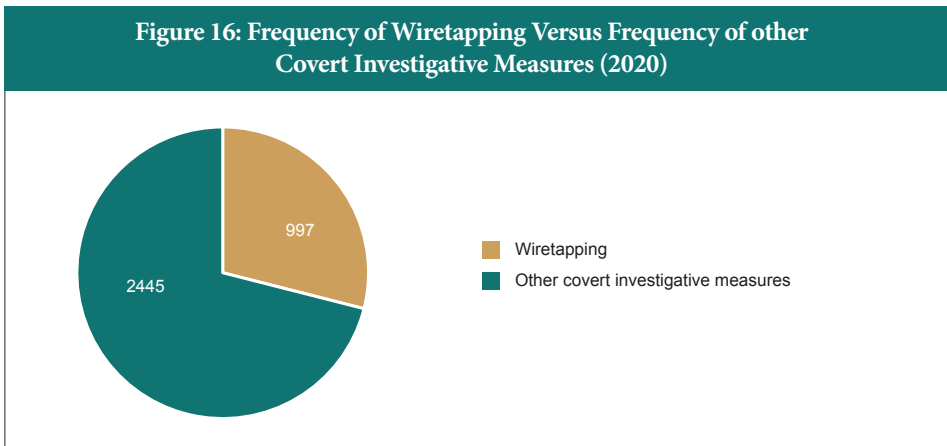
Table 5: Top Ten Most Petitioned Crimes (2021)

Definition	Judicial Review	Granted in full/partially
Membership of the ‘criminal underworld’; ‘being a thief in law’ (Article 223 ¹)	165	158
Fraud (Article 180)	145	132
Intentional infliction of serious harm to health (Article 117)	113	91
Intentional murder (Article 118)	87	78
Illegal manufacturing, production, purchase, storage, transportation, transfer or sale of drugs, their analogues, precursors or new psychoactive substances (Article 260)	87	76
Theft (Article 177)	65	50
Extortion (Article 181)	43	38
Intentional murder under aggravating circumstances (Article 109)	37	33
Legalization of illegal income (money laundering) (Article 194)	34	34
Manufacturing, sale or use of forged credit or debit card (Article 210)	34	32

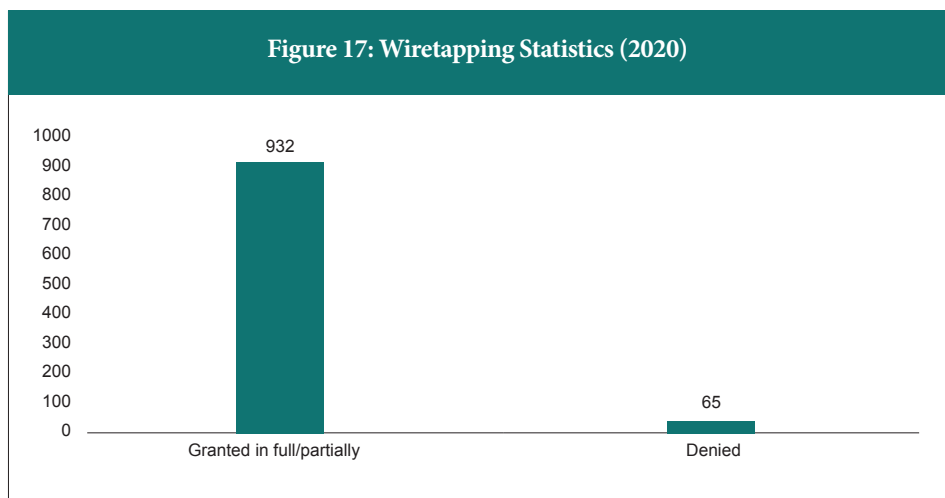
In 2020, a total of 3,442 motions regarding the use of covert investigative measures were filed in the common courts. 3274 of them were fully or partially granted constituting 95.12%.



Out of 3442 motions, 997 related to wiretapping, **which amounts to 29% of the total.**



The statistics of covert wiretapping and recording of telephone communications show that 932 out of 997 requests were fully or partially granted constituting 93.4%.

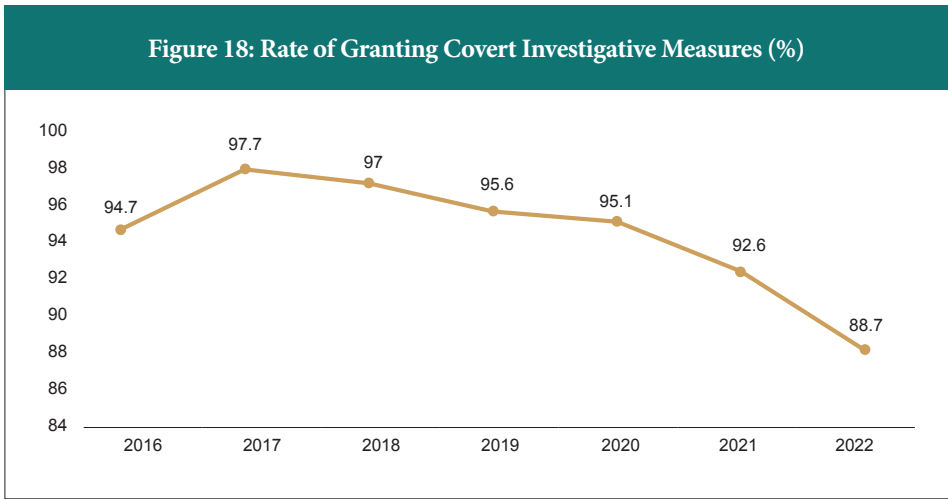


Even in 2020, covert wiretapping and recording of telephone communication was most often used in connection with the article on membership of the ‘criminal underworld’.

Table 6: 10 Crimes Regarding which most Motions were Filed (2021)

Definition	Judicial Review	Granted
Membership of the ‘criminal underworld’; ‘being a thief in law’ (Article 223 ¹)	113	107
Fraud (Article 180)	94	91
Intentional murder (Article 108)	92	86
Intentional infliction of serious harm to health (Article 117)	71	63
Illegal manufacturing, production, purchase, storage, transportation, transfer or sale of drugs, their analogues, precursors or new psychoactive substances (Article 260)	65	55
Manufacturing, sale or use of forged credit or debit card (Article 210)	50	47
Extortion (Article 181)	43	42
Theft (Article 177)	41	31
Taking bribes (Article 338)	39	39
Intentional murder under aggravating circumstances (Article 109)	28	28

Aggregate statistics from 2016-2022 show that the rate of granting investigative measures has been somewhat declining over the years but is always above 88%.

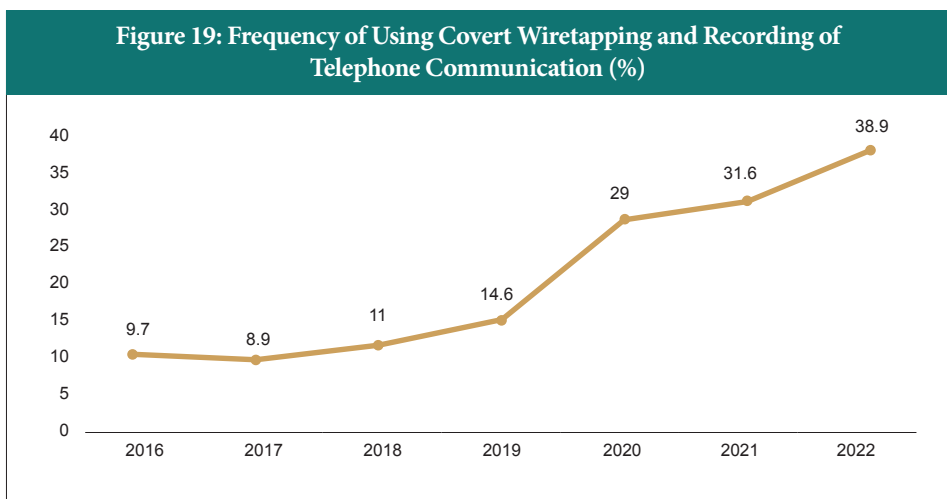


Quantitative data show that most frequently covert investigative measures were used in 2018, and the percentage of authorizations was the highest in 2017. It should be noted that since 2020, the number of motions for the use of covert investigative measures has actually halved. In addition, since 2019, the percentage of authorizations has been gradually, albeit slightly, decreasing.

Table 7: Quantitative and Percentage Indicators of Granting Covert Investigative Measures

Year	In total	Fully or partially granted	Authorization percentage
2022	3250	2882	88.7
2021	3849	3564	92.6
2020	3442	3274	95.1
2019	7084	6775	95.6
2018	9606	9317	97
2017	6157	6015	97.7
2016	4150	3929	94.7

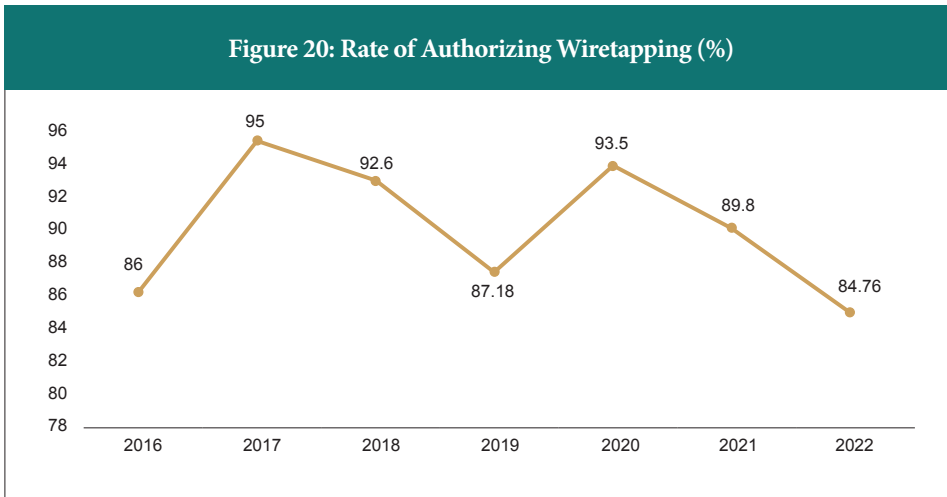
Statistical data show that the percentage of covert wiretapping and recording of telephone communications from the total number of covert investigative measures is variable, although its share is steadily increasing every year.



On the other hand, the rate of granting motions requesting covert wiretapping and recording of telephone communications varied between 84-95% in 2016-2023.

Table 8: Quantitative and Percentage Rates of Compliance with Covert Wiretapping and Recording of Telephone Communications

Year	In total	Granted in full/partially	Denied	Authorization percentage
2016	401	345	56	86
2017	548	521	27	95
2018	1059	981	78	92.6
2019	1037	904	133	87.18
2020	997	932	65	93.5
2021	1207	1089	118	89.8
2022	1266	1073	193	84.76



In total, based on the statistics for 2020-2023, it can be said that the two crimes for which covert wiretapping and recording of telephone communications were most frequently used during each of the years were membership of the ‘criminal underworld’, being a thief in law (Article 223¹) and fraud (Article 180).

2.12 Summary

This chapter reviewed the legislation regulating judicial oversight over the use of covert investigative measures and the practice of its implementation.

An analysis of the legislation reveals that judicial oversight is predominantly reactionary in nature. Specifically, a judge only reviews covert investigative measures upon the prosecutor’s submission of a motion or when a citizen appeals against such an action. The legislation approaches the monitoring process based on calendar intervals, with 90-day time frames, without incorporating the practice highlighted in academic literature and international recommendations, which advocate for dividing judicial supervision into three distinct stages: authorization, monitoring, and ex post facto verification. Consequently, apart from the potential to evaluate evidence during criminal proceedings, judicial oversight does not encompass the entire cycle of covert investigative measures. A significant portion of the process remains unregulated because the court lacks mechanisms for proactive monitoring of the surveillance process and the means to independently assess

its legality and necessity. Given the excessively long surveillance periods and notification postponements prescribed by legislation, the absence of proactive judicial oversight mechanisms significantly heightens the risks of human rights violations and using arbitrary measures by investigative authorities.

Furthermore, the judicial oversight framework essentially consists of only two actors: a judge and a prosecutor. It does not directly involve the operational-technical agency, which exclusively conducts a series of covert investigative activities under the prosecutor's direction. The legislation concerning covert investigative measures does not adequately assess the risks inherent in the technical execution of these measures by the operational-technical agency or the potential influence of the SSSG on it. Additionally, the limited involvement of the Personal Data Protection Service and the lack of transparency in judicial oversight create an environment conducive to an overly close, cooperative relationship between the court and the prosecutor's office. In such a relationship, a judge less constrained by direct public accountability may overly rely on and fail to critically evaluate the information and evidence provided by the prosecutor's office. To prevent the development of this "symbiosis," it is necessary that the judicial oversight process becomes more transparent. This could be achieved, for example, by more actively involving the Public Defender's Office or the Special Investigation Service in the oversight process.

It is important to note that the statistics published by the Supreme Court are incomplete, fail to identify the trends related to the use of covert investigative measures, and do not meet the minimum standards for transparency of judicial oversight. In addition to the flawed statistics, the Supreme Court exhibits a reluctance to provide public information, thereby hindering the possibility of civil oversight.

Thus, an analysis of the legal framework and practice reveals that while the procedure for authorization of covert investigative measures is clearly regulated, there are no proactive mechanisms for ongoing and post-completion inspection of the implementation process, leaving a significant portion of covert investigative measures beyond judicial oversight. Additionally, the legislation does not adequately address the institutional risks (such as agency being under the control of the State Security Service) and technical risks (such as the agency's ability to arbitrarily copy data) associated with the use of covert investigative measures.

Chapter 3. Judicial Oversight of Special Measures within the Counterintelligence Activities

3.1. Introduction

In addition to investigative purposes, electronic surveillance measures also serve counterintelligence purposes. Unlike the first process, where covert investigative actions are used within the framework of a criminal investigation for suspected crimes, counterintelligence activities have non-law enforcement objectives. Their main task is to protect state security from threats emanating from foreign intelligence services by identifying and preventing them. Counterintelligence activities are classified, and except in exceptional cases, the materials obtained from these activities are not accessible because they constitute state secrets. Unlike the investigative regime, the use of special measures in counterintelligence activities is not subject to the regulatory scope of the Criminal Procedure Code of Georgia. Consequently, there are few mechanisms to ensure the legitimacy and legality of the use of counterintelligence measures.

This section of the research reviews the legislation regulating counterintelligence activities and the legislative framework determining judicial oversight of the special measures used in this process, particularly electronic surveillance. It analyzes the oversight mechanisms provided by the Law of Georgia on “Counterintelligence Activities,” with a focus on the control exercised by the Supervising Judge over counterintelligence activities. Additionally, it examines the institutional structure of the system, the problem of separating powers among various agencies involved in counterintelligence activities, their broad powers, the foreseeability issues of certain special measures, and the challenges related to access to public information.

3.2. Types of Special Measures

The Law of Georgia on “Counterintelligence Activities” establishes a list of special measures used for carrying out counterintelligence activities. Unlike the criminal investigation regime, which aims to determine the probable occurrence of a punishable act, counterintelligence activity is a specialized type of activity in the security sector, focused on identifying and preventing threats against state interests originating from foreign intelligence services or individuals involved in espionage or terrorist activities.¹⁸⁵ Consequently, a different control regime operates for counterintelligence activities compared to criminal investigations, as it does not serve law enforcement purposes.¹⁸⁶

The organization and coordination of counterintelligence activities are the responsibility of the Counterintelligence Department of the SSSG.¹⁸⁷ In addition, “special services within their competence” are involved in the activities. Although the legislation does not specify additional information about these agencies, they are granted all the necessary powers to carry out counterintelligence activities.¹⁸⁸

It is noteworthy that the agencies involved in counterintelligence activities are defined not at the legislative level but by a decree of the Government of Georgia.¹⁸⁹ Special services are granted broad powers by law, which involve the restriction of many human rights, including the right to privacy. Although the government’s decree exhaustively lists the agencies and specific departments within them that are authorized to carry out counterintelligence activities, it is problematic that such authorities are not regulated at the legislative level, allowing the government to expand or narrow the list of special services at any time. Consequently, it is important that the legislation does not permit, including by the government, a broad interpretation of the norm, and that the executive authority does not have *carte blanche* to determine the agencies that may carry out counterintelligence or intelligence activities.

185 Law of Georgia “On Counter-Intelligence Activities”, article 1.

186 Ibid, subsection “a” of article 2.

187 Ibid, article 7, part 1.

188 Ibid, article 8.

189 Resolution No. 448 of the Government of Georgia dated October 5, 2017 “On Counter-Intelligence Activities” regarding the determination of the list of special services for the purposes of subsection “t” of article 2 of the Law of Georgia.

Within the framework of counterintelligence activities, special services are authorized to use special, operational, or operational-technical measures. The first category involves obtaining information about intelligence or terrorist activities originating from a foreign country, using either open or covert methods as part of operational activities.¹⁹⁰ In the second case, technical means are employed to conduct the same activities.¹⁹¹

Interestingly, the legislation does not explicitly define the nature of operational activities. For example, while operational-technical activities are defined by law as obtaining information using technical means and measures (e.g., covert listening and recording of telephone communications), only the purpose of operational activities is specified. The methods and measures involved in operational activities are not clearly outlined. In contrast, the list of operational-technical measures is exhaustively detailed in the legislation.¹⁹² However, the legislation delegates the definition of the types of operational measures to special services, making it unclear what specific activities are included.¹⁹³ This approach by the legislator allows special services to classify any measure or method aimed at gathering information to achieve their objectives as an operational activity. The only mechanism of oversight for these measures is internal agency control, as they are not subject to judicial review for legality.

Institutions within the security sector should inherently possess certain freedoms in selecting methods and measures when carrying out counterintelligence activities. However, fully delegating this authority to agencies must be viewed as a legislative shortcoming. Special services are strictly closed, centralized agencies often operating under the executive authority, with limited democratic oversight over their actions. Additionally, the acts that determine the types of operational measures employed by these agencies are not public. Consequently, this lack of transparency makes the regulation unforeseeable and fails to inform targeted individuals about the measures that may be applied to them within the framework of counterintelligence activities. Under such unchecked conditions, special services could incorporate any measure into counterintelligence activities that significantly interferes with human rights, justifying it under the pretext of security

190 Law of Georgia “On Counter-Intelligence Activities”, article 9, part 1, subsection “a”.

191 Ibid, subsection “b”.

192 Ibid, part 2.

193 Ibid, part 1, subsection “a”.

protection.

As previously mentioned, the legislation exhaustively defines the list of operational-technical measures. To collect information, special services are authorized to use methods such as:

1. Covert video and audio recording;
2. Covert cinema and photo shooting;
3. Use of television cameras and other electronic devices;
4. Electronic surveillance;
5. Control of postal correspondence;
6. Strategic monitoring;
7. Individual monitoring measures.¹⁹⁴

The legislation specifies that electronic surveillance includes three types of measures:

1. Covert listening and recording of telephone communications;
2. Extraction and recording of information from communication channels;
3. Real-time geolocation determination.¹⁹⁵

Most of these measures are also used for covert investigative actions and have the same meaning. However, there are three special methods that, according to the legislation, are employed exclusively within the framework of counterintelligence activities:

1. Use of television cameras and other electronic devices;
2. Individual monitoring;
3. Strategic monitoring.

These types of measures are not included in the list of covert investigative actions. In the first case, the legislator grants the head of the special service the authority to issue consent for the use of television cameras and other electronic devices in public gathering places.¹⁹⁶ It is unclear what exactly this specific measure entails.

¹⁹⁴ Ibid, article 9, part 2.

¹⁹⁵ Ibid, article 4, part 3.

¹⁹⁶ Ibid, article 17.

The norm does not specify the electronic devices that subjects involved in counterintelligence activities are permitted to use. Such an approach may imply that in public gathering places, special services could potentially use any individual's electronic devices (phones, computers, etc.) for counterintelligence purposes. The legislation also mentions the use of television cameras, which presumably includes equipment from broadcasters. However, it remains unclear how these devices are to be used and whether their use could involve, for example, extracting specific information. Additionally, it is not specified whether special services need the owners' permission or consent to use their electronic devices for counterintelligence purposes.

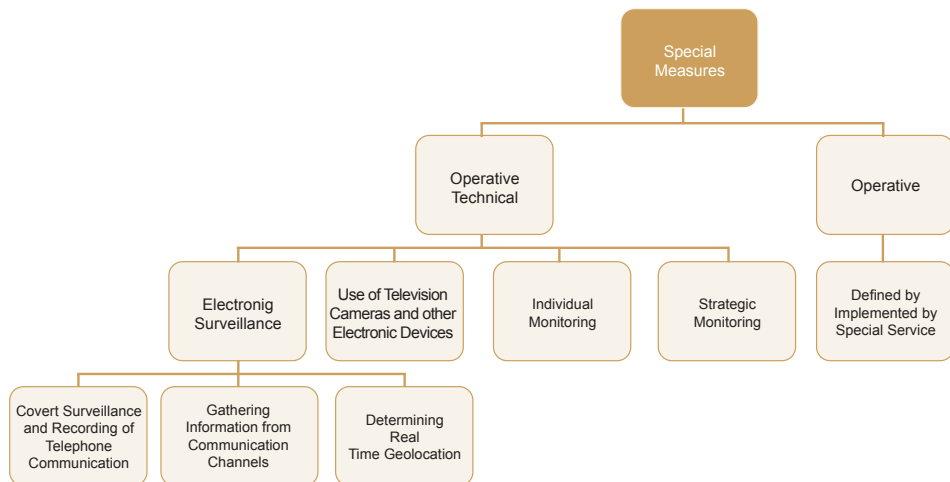
Along with this ambiguity, it is problematic that such norms lack effective oversight, and the only person authorized to decide on the use of these measures is the head of the special service. This reveals another legislative flaw. Specifically, according to the Law on Counterintelligence Activities, a special service is defined as an agency or a relevant unit within an agency authorized by government decree to use special counterintelligence measures. For instance, the SSSG, as a separate agency, is not considered a special service for counterintelligence purposes; only certain departments within it are authorized to conduct counterintelligence activities. Therefore, when the legislation refers to the head of the special service as the person granting the permit, it does not clarify whether this refers to a political office holder, such as the head of the SSSG or the Minister of Internal Affairs, or to the head of a department designated as the special service, such as the head of the Counterintelligence Department of the SSSG. This legislative wording suggests that the consent for carrying out special measures is issued not by the highest authority of the institution (e.g., Ministry of Internal Affairs, SSSG) but by a specific unit (e.g., Counterintelligence Department), i.e., by the head of a specific department.

The meaning of individual and strategic monitoring is defined by the Law on the Operational-Technical Agency of Georgia. The first type of special measure involves monitoring telecommunication messages transmitted through electronic communication networks using the technical identifier of specific communication equipment located outside the territory of Georgia or in areas where Georgian jurisdiction does not apply.¹⁹⁷ The second measure, following the same princi-

¹⁹⁷ Law of Georgia "On Legal Entity of Public Law - Operative-Technical Agency of Georgia", article 2, subsection "b".

ple, involves monitoring the general telecommunication flow rather than specific messages.¹⁹⁸ The legislation does not provide additional information on these two measures. Therefore, it is assumed that the first measure refers to targeted monitoring, which involves controlling telecommunication messages related to specific individuals. In contrast, the second measure likely involves general telecommunication monitoring, where representatives of the special service monitor the flow of messages, strategically searching for interesting and useful information based on themes and content. The general objective of these two special counterintelligence measures is to obtain information about actions directed against Georgia's constitutional order, sovereignty, defense capability, territorial integrity, public order, and scientific, economic, and military potential.

Figure 21: Types of the Operational-Technical Measures



198 Ibid, subsection “b”.

3.3. Agencies Authorized to Conduct Special Measures

The agencies authorized to conduct intelligence and counterintelligence activities in Georgia are delineated by a decree of the Government of Georgia. The complexities and issues related to regulating these activities through subordinate normative acts have been discussed in a preceding subsection of this document. The specific list of special services endowed with the authority to conduct counterintelligence activities was established by the Government's decree on October 5, 2017. The primary agencies tasked with detecting and preventing threats against the state's interests are the SSSG MIA of Georgia.¹⁹⁹

Furthermore, the government grants the authority to conduct individual and strategic monitoring measures to the Georgian Intelligence Service and the Military Intelligence Department of the Ministry of Defense's Defense Forces. The decree provides an exhaustive list of the structural units within the SSSG and the MIA that are authorized to employ special measures as part of their intelligence and counterintelligence activities. These units are formally designated as special services under the Law on Counterintelligence Activities. The specific units include:

For the SSSG:

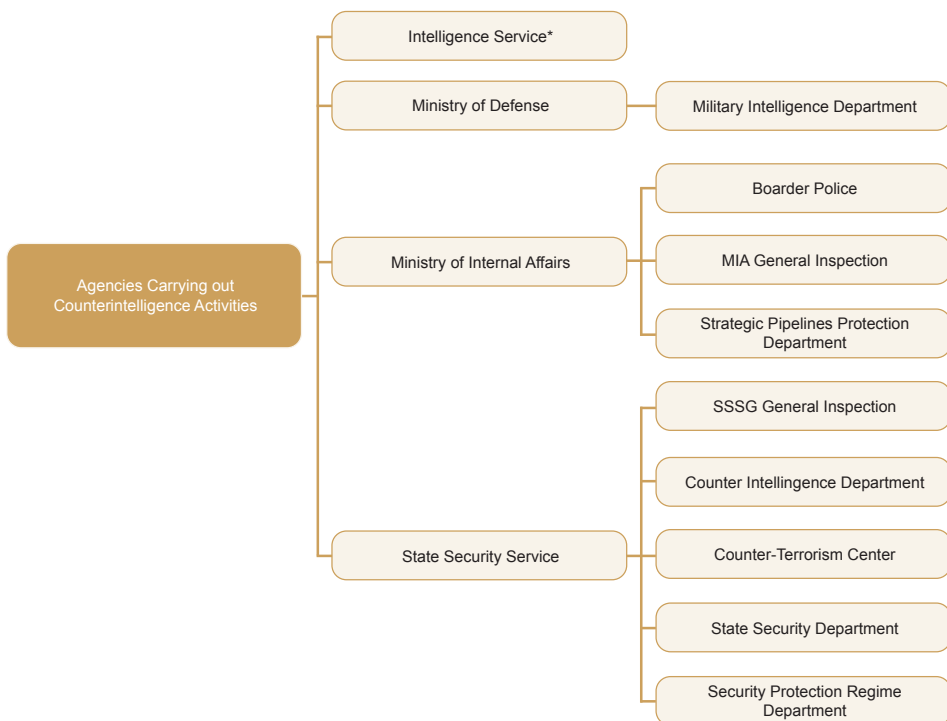
1. General Inspection
2. Counterintelligence Department
3. Counterterrorism Center
4. State Security Department
5. Security Protection Regime Department

For the MIA:

1. General Inspection
2. Strategic Pipelines Protection Department
3. Georgian Border Police

199 Resolution No. 448 of the Government of Georgia dated October 5, 2017 "On Counter-Intelligence Activities" regarding the determination of the list of special services for the purposes of subsection "t" of Article 2 of the Law of Georgia.

Figure 22: Special services authorized to carry out counterintelligence activities²⁰⁰



3.4. Competencies of Special Services and the Problem of Duplication of Powers

The legislation grants special services involved in counterintelligence activities broad powers. Beyond their counterintelligence functions, these agencies frequently exercise investigative authority as well. This section of the study outlines the competencies of these special services and examines the issue of overlapping authorities among them.

200 Note: Within the framework of counterintelligence activities, the Georgian Intelligence Service and the Military Intelligence Department of the Georgian Ministry of Defense's Defense Forces are only authorized to conduct strategic and individual monitoring measures.

The Counterintelligence Department of the SSSG is responsible for coordinating and organizing counterintelligence activities.²⁰¹ This structural unit is equipped with coordinating, analytical, and investigative functions. Its primary role involves conducting counterintelligence activities, including detecting, preventing, and countering actions undertaken by foreign representatives against Georgia.²⁰² Additionally, it carries out operational-search measures as provided by law, employs procedural coercive measures, and investigates criminal cases within its jurisdiction.²⁰³ The functions of the Counterintelligence Department also encompass the development and implementation of measures to protect state secrets, monitoring the execution of these measures, and vetting individuals granted access to classified information.²⁰⁴ As a result, the Counterintelligence Department is endowed with a wide range of powers.

In contrast, the functions of the Counterterrorism Center are more narrowly defined, with its primary responsibility being the combatting of terrorism. The Center exercises this authority through both investigative and preventive measures. Additionally, the Counterterrorism Center is authorized to conduct operational-search measures and investigate criminal cases within its jurisdiction.²⁰⁵

Another agency involved in counterintelligence activities is the State Security Department of the (SSSG). This department is tasked with protecting the country's territorial integrity, constitutional order, and sovereignty, as well as preventing unconstitutional and violent changes to the state constitutional system and government.²⁰⁶ Its competencies include forecasting, detecting, and countering political and economic threats. The State Security Department is responsible for both collecting and analyzing information, as well as investigating and preventing crimes within its jurisdiction. According to the legislation, its jurisdiction extends to investigating crimes directed against the state or those involving signs of extremism. However, the concept of a crime "containing signs of extremism" is not explicitly defined in the Criminal Code. As a result, it is challenging to ascertain which specific actions fall under the jurisdiction of the

201 Resolution No. 385 of the Government of Georgia of July 30, 2015 "On Approving the Regulations of the State Security Service of Georgia", Article 7, subparagraph "g".

202 Ibid.

203 Ibid.

204 Ibid.

205 Ibid, subsection "k".

206 Ibid, subsection "t".

State Security Department, aside from crimes directed against the state, such as espionage or the disclosure of state secrets.²⁰⁷

All three departments – the Counterintelligence Department, the Counterterrorism Center, and the State Security Department – are involved in detecting, preventing, and countering crimes directed against the state. Consequently, they possess not only analytical but also counterintelligence and investigative functions. A generalized analysis of the activities of these SSSG departments reveals internal institutional challenges, including overlapping authorities among the structural units. For instance, it remains unclear what specific types of crimes the State Security Department can investigate, given that nearly the entire list of state-directed crimes falls under the jurisdiction of the Counterterrorism Center and the Counterintelligence Department.

Although counterintelligence activities are primarily non-law enforcement in nature, the legislation permits instances where information obtained during counterintelligence operations can be utilized for investigative purposes. In addition to strategic and individual monitoring measures, any information acquired during special measures may be transferred to an investigative body to initiate an investigation of a suspected crime or to support an ongoing investigation.²⁰⁸ The decision to transfer information obtained during counterintelligence activities to an investigative body is made by the head of the special service. However, the specific criteria governing this decision remain unclear. Such criteria might include the relevance of the information to the investigation, the urgent need to protect national security, or the necessity of investigating a crime for which covert investigative actions are permissible.²⁰⁹

As a result, the aforementioned departments of the SSSG are able to employ special measures for counterintelligence purposes, including those not subject to judicial oversight. Simultaneously, they can utilize the information obtained to investigate crimes within the SSSG's jurisdiction. This blending of law enforcement and non-law enforcement functions renders the SSSG's powers largely unchecked and creates a significant risk that information gathered during counterintelligence activities could be repurposed for investigative purposes without adhering to the

207 Law of Georgia “Criminal Code of Georgia”, Chapter 11.

208 Law of Georgia “On Counter-Intelligence Activities”, article 14⁸.

209 Ibid.

evidentiary standards required for covert investigative actions. This risk is further exacerbated by the existence of nearly identical measures in both the counterintelligence and investigative regimes. The primary distinction in their application lies in the investigative regime, where any covert action necessitates meeting evidentiary standards and obtaining a court warrant. Judicial oversight in the counterintelligence regime is limited, primarily applying only to electronic surveillance mechanisms.

In addition to these three departments, the Security Protection Regime Department of the SSSG is responsible for counterintelligence activities, establishing security regimes for high-risk subjects to state security, and identifying threats against them.²¹⁰

Two main institutions within the Ministry of Internal Affairs (MIA) are involved in counterintelligence activities: the Border Police and the Strategic Pipelines Protection Department. The Border Police is responsible for protecting the state border and maritime space, ensuring the territorial integrity, inviolability of the borders, and security of the state, citizens, and their property in cooperation with other agencies.²¹¹ The main function of the Strategic Pipelines Protection Department is to protect and ensure the security of strategic pipelines and their infrastructure facilities passing through the country's territory.²¹²

The government decree additionally designates the General Inspections of the SSSG and MIA as subjects conducting counterintelligence activities. These structural units serve as internal control mechanisms for the agencies.²¹³

The functions of the structural units, particularly those within the SSSG, are often general and duplicative. It is also important to note that besides the order of the General Prosecutor of Georgia, which determines the investigative and territorial investigative

210 Resolution No. 385 of the Government of Georgia of July 30, 2015 "On Approving the Regulations of the State Security Service of Georgia", Article 7, subsection "T1".

211 Order No. 786 of the Minister of Internal Affairs of Georgia dated June 21, 2006 "On approval of the regulations of the state sub-departmental institution of the Ministry of Internal Affairs of Georgia - Border Police of Georgia", article 4.

212 Resolution No. 337 of the Government of Georgia of December 13, 2013 "On Approving the Regulation of the Ministry of Internal Affairs of Georgia", article 10, subsection "N3".

213 Resolution No. 385 of the Government of Georgia of July 30, 2015 "On Approving the Regulations of the State Security Service of Georgia", article 50, part 4.

jurisdiction of criminal cases, publicly available normative sources do not include an order of the head of the SSSG or another subordinate normative act that would determine the distribution of investigative functions among the SSSG departments. Furthermore, the regulations of the SSSG departments involved in counterintelligence activities or conducting special measures are not publicly available. In other cases, the regulations of structural units are publicly accessible.²¹⁴

A structural unit's regulation cannot be entirely classified, as it contains significant public information such as the department's legal structure, organization, primary tasks, and general competencies. While counterintelligence activities are classified by law, this does not imply that the public should be denied access to essential public information about these departments. The departments of the SSSG also perform functions beyond counterintelligence, which fall under the criminal law regime. Moreover, the law sets a standard for classifying information, stipulating that such a status should be granted only when it is necessary to protect state or public security or judicial interests in a democratic society.²¹⁵ Additionally, it is necessary to substantiate the harm in the process of classifying any information.

Therefore, it is crucial that special services involved in counterintelligence activities adhere to at least a minimum standard of transparency. This level of transparency should not impede their operations nor compromise public and state security. Such information should include general data regarding the structure, organization, tasks, and working principles of these departments, all of which should be grounded in the constitution and the current legislation governing the security sector.

3.5. Target Objects of Special Measures

Unlike covert investigative actions, where the circle of subjects depends on the circumstances identified within the framework of the investigation, the concept of an object of counterintelligence activity is much broader. According to the legislation, counterintelligence activities are carried out to achieve a specific goal and do not have a law enforcement function. Consequently, the target object of special measures can be any person who may pose a threat to the counterintelligence

214 The Website of the State Security Service, available at: <https://cutt.ly/kwBhd5Gx>, Updated: 19.02.2024.

215 Law of Georgia "On State Secrets", article 2¹.

body due to intelligence or terrorist activities directed against the state interests of Georgia by foreign special services, organizations, groups of individuals, or individual persons.²¹⁶

Special services are authorized to carry out counterintelligence activities against any person, regardless of their citizenship, nationality, gender, official position, place of residence, membership in a public association, religious belief, or political conviction.²¹⁷ The only restriction established by the legislation is related to the location of the counterintelligence activities. Special services have such authority only within the territory of Georgia.²¹⁸ Therefore, unlike criminal proceedings, the counterintelligence regime allows special services to use certain special measures against any person without justification.

The legislation establishes the following grounds for the implementation of special measures:

- Data about facts and events, or their signs, that threaten or may threaten the state security of Georgia;
- Data about a foreign representative or a representative office of a foreign country related to intelligence or terrorist activities, preparation or implementation of actions directed against the state security interests of Georgia, or the existence of grounds for such an assumption;
- Data about a Georgian person indicating their connection with the intelligence or terrorist activities of foreign special services.²¹⁹

The grounds proposed by the legislation for the implementation of counterintelligence activities are general and indeterminate. The legislation does not define some terminology. For example, it is not known what type of data/information may be sufficient to implement special measures. Besides facts and events, it is unclear what is meant by the presence of signs of actions directed against state interests. Additionally, the legislation allows for actions not based on facts and data but introduces the assumption that a specific person or organization, through their activities, may be preparing or carrying out actions directed against state security

216 Law of Georgia “On Counter-Intelligence Activities”, article 1.

217 Ibid article 11, part 1.

218 Ibid.

219 Ibid, article 10.

or related to terrorism. Such a general and vague definition of grounds creates a risk in each individual case that the counterintelligence body will determine for itself what type of activities, facts, events, or persons are considered a threat to state security. It is clear that the language of the legislator grants special services all kinds of freedoms to include any person, organization, action, or event within the scope of counterintelligence activities and to create legal grounds for using intensive measures that interfere with human rights. This approach makes the conduct of rights-restricting measures “formally legal,” but the proportionality and legitimacy of these measures are in question.

Under conditions where it is sufficient to carry out most special measures based solely on the order of the head of the special service, and most of these measures are not subject to democratic control mechanisms, the existence of such broad definitions of grounds is even more problematic. Such a general definition grants wide discretion to the counterintelligence bodies, and under an ineffective oversight system, there is a risk that special services will use their power disproportionately and illegitimately.

3.6. Procedure for Conducting Special Measures and Judicial Oversight

Despite the fact that the special measures carried out within the framework of counterintelligence activities provide for intensive interference in a person’s personal life of various natures, unlike the investigative regime, democratic control mechanisms, especially judicial control, do not apply to a large part of the activities. The legislation clarifies that counterintelligence agencies have minimal restrictions on the use of special measures and require court authorization in only two cases - electronic surveillance and postal correspondence control.²²⁰

As already mentioned, electronic surveillance and control of postal correspondence belong to a number of operational-technical measures. It is worth noting that, on the one hand, the judicial control mechanism does not include a complete list of operative-technical measures (for example, covert video-audio recording, covert film-photographing, individual and strategic monitoring), which may not be identical, but no less intensively encroach on basic human rights. and free-

²²⁰ Ibid, subsections “a” and “b” of article 11.

doms. On the other hand, judicial control does not apply to operational measures, the types of which are determined by legal acts of special services and are not regulated by law. Consequently, both the decision to use them and their execution can be the only means of control by internal departmental mechanisms.

Although legislation regulates judicial oversight over electronic surveillance and postal correspondence monitoring, operational-technical measures carried out within the framework of counterintelligence activities are not subject to procedures established for criminal justice processes and law enforcement purposes. The “Law on Counterintelligence Activities” designates a supervising judge with appropriate authority, who is the only one capable of effectively controlling the measures carried out by special services. The supervising judge is a member of the Supreme Court of Georgia, appointed by the Chairperson to review the legality of specific operational-technical measures conducted within the scope of counterintelligence activities.²²¹

The legislation does not specify the procedure by which the Chairperson of the Supreme Court selects the supervising judge from among the court’s members. Furthermore, there is no information available regarding the specific qualifications required to exercise these powers, particularly in the technical oversight of electronic surveillance. The only situation in which the supervising judge is replaced occurs when they are unable to fulfill their assigned duties for any reason; in such cases, another judge from the same court, appointed by the Chairperson of the Supreme Court, assumes the role.²²²

Although the “Law on State Secrets” or its annex, which defines the list of information classified as state secrets, does not indicate the possibility of keeping the identity of the supervising judge secret, the identity of the judge entrusted with these powers by the Chairperson of the Supreme Court is not publicly known. The only basis for keeping the identity of the supervising judge secret is likely the general norm defining the classified nature of counterintelligence activities.

According to Georgian legislation, judicial oversight over counterintelligence activities is implemented through three mechanisms: *ex ante* supervision, process monitoring, and *ex post* supervision. In the first case, similar to the

221 *Ibid*, subsection “u” of article 2.

222 *Ibid*, article 14⁶, part 5.

investigative regime, the judge issues an order for electronic surveillance measures upon the satisfaction of a motion submitted by the special service. In the second case, the judge directly controls the surveillance process using special technical means and proactively requests information from the special services about the measures conducted. In the third case, special services conduct counterintelligence activities without prior judicial authorization under urgent necessity, and subsequently seek the judge's review of the legality of the actions already taken.²²³

It is commendable that the supervising judge has the authority to oversee both the technical and substantive aspects of electronic surveillance during the process. On one hand, the judge utilizes special electronic means to verify that the actions of the special services align with the order issued and its specific requirements. On the other hand, the judge can request the special service to provide information about the ongoing electronic surveillance and the data obtained from it. The judge may review this information in a closed session with the participation of a representative from the special service. If it is determined that legal grounds for termination or suspension exist, the judge has the authority to terminate the electronic surveillance.²²⁴

Legislation further specifies the grounds for terminating or suspending special measures. Electronic surveillance is terminated if the specific task outlined in the supervising judge's order has been completed, the surveillance period has expired, continuing the measure objectively cannot achieve the set goal, or continuing surveillance is no longer significantly important for obtaining information.²²⁵ The supervising judge has the authority to suspend electronic surveillance using the electronic system if it is conducted without the judge's order or if there is no electronic copy of the special service head's decision in the case of urgent necessity.²²⁶

This legislative arrangement suggests that the grounds for terminating electronic surveillance are largely formal. As a result, the supervising judge primarily verifies whether the measure adheres to the formal criteria established by law, such as the judge's authorization or, in urgent cases, the decision of the special service head.

223 Ibid, articles 14, 13, 14⁵ and 14⁶.

224 Ibid.

225 Ibid, part 14⁴, part 1.

226 Ibid, part 4.

The role of the supervising judge can be likened to the authority of the head of the Personal Data Protection Service in the investigative regime, where they oversee the legality of covert investigative actions using a special electronic system. However, when it comes to the grounds for termination, the supervising judge plays a more significant role in analyzing the substantive aspects of counterintelligence activities. Notably, the legislation does not require the supervising body itself to evaluate whether the objective specified in the judge's order has been achieved before the deadline. Instead, this responsibility falls to the head of the special service, who, as an interested party, is the one who initially requests the court's authorization for electronic surveillance.²²⁷ Different regulation applies when it concerns the early termination of electronic surveillance based on the importance and necessity of the obtained information. In this case, apart from the head of the special service, the supervising judge also has the authority to terminate the special measure.

Such regulation conflicts with the general principles of judicial oversight. Firstly, the legislation effectively equips the head of the special service with the functions of a supervisory judge. When using electronic surveillance, they approach a judge to request permission to carry out measures for a specific task, which the court then reviews to assess the legality and legitimacy of the request. However, when it comes to prematurely terminating surveillance, it is not the judge but the head of the special service who evaluates whether the task defined by the supervisory authority's order has been completed. This model contradicts the logic of judicial oversight and renders the judge's tool to prematurely terminate electronic surveillance ineffective; preventing the judge from evaluating the completion of the task, they initially defined.

The third basis for possible termination of electronic surveillance relates to the expiration of the supervisory judge's order. If the period defined by the order for implementing the special measure has expired, the electronic surveillance will be stopped. According to the legislation, an order for electronic surveillance is issued for a period necessary to achieve the set goal, but no longer than 90 days.²²⁸ In this case, the problematic aspect is not the 90-day maximum period itself, but the norm regulating its extension. Specifically, the 90-day period can be extended based on a motivated request in the same manner and on the same grounds as the

²²⁷ Ibid, part 2.

²²⁸ Ibid, article 13, part 4.

original order, for no more than 12 months each time.²²⁹ There is no restriction on how many times the special service can approach the supervisory judge with a request. Consequently, electronic surveillance can continue indefinitely as long as the judge considers the request for extension justified, or until another legal basis for termination arises, whose ineffectiveness is discussed in the paragraph above.

As a result, judicial oversight is ineffective in suspending and terminating electronic surveillance, largely due to the increased involvement of special services in the decision-making process. These services assess the completion of counterintelligence tasks without judicial involvement and can independently decide on the premature termination or indefinite continuation of electronic surveillance. Although the supervising judge has the authority to request written explanations from the competent authority on specific issues identified during the oversight process and can make decisions based on interim reports, their power to terminate electronic surveillance is limited to two scenarios: when the interim report unequivocally demonstrates that achieving the counterintelligence goal through electronic surveillance is objectively impossible, and when considering a request to extend the surveillance period. Importantly, the judge cannot terminate the special measure based on the completion of the counterintelligence task as defined in the initial order; this authority is granted exclusively to the head of the special service. When it comes to suspending electronic surveillance, the supervising judge's role is confined to addressing formal-legal and technical issues, such as verifying the existence of the order and ensuring the accuracy of logging data.²³⁰

There are other subjective and objective challenges that weaken such tools in practice. For example, substantive control of the electronic surveillance process is at the discretionary authority of the judge, and they are not obliged to request information from the special services about ongoing actions and review whether there are legal grounds for suspending or terminating counterintelligence activities. In this process, the judge is entirely dependent on the information and materials provided by the special service. They do not have additional means to verify the accuracy of the submitted materials, which form the basis for the request for electronic surveillance. Consequently, the supervisory judge bases their decision entirely on unilaterally obtained information, as they do not have the opportunity to consider other, differing arguments or data. This problem is exacerbated by

229 Ibid, part 5.

230 Ibid, article 14⁶, part 5.

the fact that the legislation does not define the necessary qualifications for the supervisory judge to exercise their authority. Among other things, the judge is not required to have knowledge of national security issues. In such an arrangement, it is likely that the supervisory judge will become more vulnerable to the security argument and will not engage in detailed analysis during the review of the request, as they lack the competence and access to alternative sources of information that could counter the argument presented by the special service.

Unlike the investigative regime, the supervisory judge also oversees the formal-legal and technical control of counterintelligence activities. Accordingly, they verify the compliance of the order with the electronic surveillance measures conducted by the special services. In the investigative regime, the head of the Personal Data Protection Service holds this function. It is desirable that a third, independent institution be involved in the oversight process of counterintelligence activities, similar to the control of covert investigative actions.

The acting supervisory judge for electronic surveillance is always one person, determined by the sole decision of the Chairperson of the Supreme Court. It is preferable that such decisions be made not by one, but by several judges, based on the principle of rotation. The legislation does not define the term for combining the functions of the supervisory judge, and therefore, given this legislative arrangement and the principle of lifetime appointment of Supreme Court judges, it is possible that the supervisory judge will be one person for many years. This raises the risk that the judge will become more vulnerable to the security argument and will consider the requests for electronic surveillance measures subjectively, as they do not have the means to obtain alternative information and hear arguments unilaterally. Although it was noted that reviewing such requests requires special competence, introducing the rotation principle will not significantly increase the pool of judges who will have to review such requests and have access to state secrets. This is primarily due to the fact that the jurisdiction to review requests for electronic surveillance measures within the framework of counterintelligence activities belongs to the Supreme Court of Georgia, which is composed of high-legitimacy members.

In summary, judicial oversight of counterintelligence activities suffers from several fundamental flaws. One major issue is the limited scope of measures subject to judicial oversight. Even when the court has tools to oversee certain operational-technical measures, it lacks the resources and legal mechanisms to conduct independent investigations or obtain additional information that could inform its decisions. This lim-

itation creates a risk that the judge will consistently rely on the unilateral information provided by the special services and make decisions in favor of the security argument. Given the secrecy surrounding counterintelligence activities, the process of reviewing motions cannot adhere to the principle of adversarial proceedings, making the judge's role crucial in ensuring fairness when analyzing submitted materials. Moreover, the supervisory judge lacks the authority to independently suspend electronic surveillance measures ahead of schedule if they believe the counterintelligence objective has been achieved. The notification mechanism for the individual is also inadequate, as it relies heavily on the good faith of the head of the special service.

Another challenge is the legislation's provision for only temporary replacement of the judge overseeing electronic surveillance motions, limited to situations where the designated supervisory judge is physically unable to perform their duties. It would be more effective if the legislation allowed for rotation among several Supreme Court judges when reviewing such significant matters, which would reduce the judge's vulnerability to pressure from special services during the motion hearing process.

3.7. Problem of Access to Statistical Information

Both special services and the Supreme Court of Georgia use the argument of the secretive nature of counterintelligence activities to restrict access to information that is unequivocally public, regardless of its relevance to counterintelligence matters. For example, various types of statistical data are classified simply because they are associated with counterintelligence activities, even when disclosing such information would not reveal the content, methods, involved services, or individuals related to those activities.

For instance, the Supreme Court does not maintain statistics on the use of electronic surveillance measures, arguing that such activities are classified as counterintelligence. On January 14, 2022, the Social Justice Center requested from the Supreme Court statistics on the approvals of electronic surveillance conducted in 2021, including the number of individuals subjected to surveillance based on the issued orders and the duration of the surveillance. The court declined to provide this information, citing the confidentiality of counterintelligence activities.²³¹

231 Decision No. z-25-22 of February 23, 2022 of Giorgi Gegelia, Acting Manager of the Supreme Court of Georgia, on refusal to satisfy the administrative complaint.

The legal dispute over the refusal to provide this information is ongoing with the Supreme Court. According to Georgian law, in the process of classifying information, it is important to apply the harm test and justify why the security argument outweighs the right to access public information, and what harm will be done to state welfare if the specific information is disclosed. The fact that specific information is related to counterintelligence activities does not automatically mean it is classified, if such information does not describe the content of special measures and does not harm state interests. Statistical information does not allow for the analysis of whom or under what circumstances electronic surveillance measures were carried out. Moreover, it is impossible to determine the content of counterintelligence activities from statistical information alone. The only information such data would provide to the public is a general understanding of the frequency, intensity, and duration of counterintelligence activities by the state, thereby giving an overview of the state's security policies.

Notably, later on, the SSSG itself included statistical data on electronic surveillance in its activity report. According to the report, in 2022, the court issued similar orders 33 times.²³² However, this statistic is also incomplete and does not answer all the questions existing in society, such as how many times in total the special service approached the court with motions, in how many cases the motions were not granted or were partially granted, how many individuals were subjected to electronic surveillance under the 33 orders, and for how long. An example of inconsistent practice in maintaining statistics is that, unlike the 2022 activity report, the document registered in Parliament in 2023 no longer separates data on electronic surveillance conducted within counterintelligence activities. According to the report, in 2023, a total of 1,933 warrants/orders and 53 motivated resolutions by the prosecutor were presented in the agency for the purpose of conducting urgent secret investigative actions and electronic surveillance measures, which does not allow for differentiation of how many times the agency used electronic surveillance measures for investigative and counterintelligence purposes.²³³ The severity of the problem is highlighted by the fact that despite the public nature of the aforementioned data, the SSSG still does not provide statistical information to the Social Justice Center as public information. In response to the February 21, 2024 letter, in which the organization requested statistics on the orders issued by the supervisory

232 2022 Report of the State Security Service of Georgia, p. 33, Available at: <https://cutt.ly/QwBhbqV>, Updated: 19.02.2024.

233 2022 Report of the State Security Service of Georgia, p. 42, Available at: <https://cutt.ly/Hw58x-KYy>, Updated: 22.04.2024.

judge in 2020-2023, the SSSG stated that counterintelligence activities are classified and that the obligation of publicity does not apply to information related to operational-search activities according to the General Administrative Code.²³⁴

Proper processing of such information would allow society to assess, on the one hand, the scale of electronic surveillance measures used within counterintelligence activities and also to discuss the effectiveness of court oversight based on the approval rate.

Alongside the concealment of statistics, the mechanism for notifying an individual about the implementation of electronic surveillance is also problematic. Despite the fact that special services are obliged to inform an individual about electronic surveillance conducted against them, the law leaves the decision entirely up to the initiator, i.e., the head of the special service. They must decide whether such notification poses a threat to national security and the protection of democratic order interests, the disclosure of information obtained as a result of electronic surveillance or the methods used to obtain it, or the objectives defined by counterintelligence activities.²³⁵ As a result, by decision of the special service, the individual may never become aware of the electronic surveillance conducted against them. Another problematic aspect in this regard is that the law does not establish a timeframe within which the individual must be notified. Under such legal regulations, the notification mechanism is ineffective, and even when it is possible to challenge the implementation of electronic surveillance, the subject of counterintelligence activities cannot appeal to the court if the special service decides that notification poses a threat to the state. This, in turn, raises the risk that counterintelligence agencies may always use this argument when they consider that there may be a real basis for challenging the electronic surveillance measures they have conducted and may withhold such information from the surveillance subjects. This decision lacks a control mechanism since the law does not establish a standard or obligation for justification, nor any form of democratic oversight mechanism to verify how legitimately the special service withheld information from the individual regarding electronic surveillance conducted against them.

234 Letter of the State Security Service of Georgia dated March 7, 2024 SSG 2 24 00053786.

235 Law of Georgia “On Counter-Intelligence Activities”, article 14¹⁰.

3.8. Summary

The secret nature of counterintelligence activities stems from their objectives. They serve the state's security and aim to protect it from external threats. Nevertheless, it is important that the systemic organization of the security sector adheres to the standards of accountability and transparency that align with the nature of such institutions' activities. The complete secrecy of such a closed system poses the risk that its vast power and capabilities could be turned into a political weapon in the hands of an unscrupulous authority. Therefore, it is crucial that, alongside protecting national interests, the legislation provides for mechanisms of democratic control over the security sector, which would prevent the misuse and illegitimate use of powers by special services.

The analysis of legislation regulating counterintelligence activities reveals several significant problems. The bases for implementing special measures provided for by counterintelligence activities are general, broad, and opaque. With such definitions, special services can justify conducting counterintelligence activities in any case, even when there is no objective need. In turn, many of the special measures are inadequately defined in the legislation, making it impossible to assess the extent to which these measures interfere with basic human rights and whether they require higher standards of control. Another issue is that, unlike investigative regimes, most special measures implemented within counterintelligence activities, except for electronic surveillance and postal correspondence, do not require a court warrant. Unlike operational-technical measures, the legislation does not define the types of operational measures and entrusts the preparation of their list to special services based on internal, secret acts. It is also not established what standards operational activities must meet to avoid intense interference with human rights. Consequently, it is hypothetically possible that the types of operational activities developed by special services could be more intense than, for example, electronic surveillance, which requires judicial control even under similar regulations.

The decision to conduct special measures, if not subject to judicial control, is made solely by the head of the special service. Another issue is that the head of the special service is defined as the head of the counterintelligence department within the SSSG or MIA, rather than the head of the respective agency. The list of special services is long and is defined not by law but by a subordinate normative act, a government decree. This arrangement allows the government to increase or

decrease the list of agencies authorized to conduct counterintelligence activities without any additional justification, equipping many state bodies with the uncontrolled functions of counterintelligence agencies. Among the SSSG agencies authorized to conduct counterintelligence activities, the division of powers is problematic. It is unclear how their functions are divided concerning the investigation of different crimes. A significant risk is that these agencies are equipped with both counterintelligence and investigative functions, raising the possibility that they could use special measures when there is no standard of proof for conducting covert investigative actions as defined by the Criminal Procedure Code. In such cases, special departments within the SSSG could use measures not subject to judicial control and later use this information for investigative purposes. This is facilitated by the fact that the SSSG is responsible for investigating crimes against the state.

Even when a specific special measure requires judicial control, the oversight system is inadequate and ineffective. In this regard, the procedure for appointing the supervising judge is particularly noteworthy. It does not meet the minimum standards of transparency and accountability, as the decision to appoint the judge is made unilaterally by the Chief Justice of the Supreme Court. There is no principle of rotation among judges, and under the conditions of lifetime appointment, one person could oversee counterintelligence activities for years without change. This situation also raises the risk that, considering the power held by the security sector, the judge could become personally vulnerable or, given limited qualifications and access to information, be inclined to favor security arguments.

Even within the existing legislative model, where the judge has three types of control over electronic surveillance (ex-ante, during the process, ex-post), the available oversight mechanisms are ineffective. For example, the judge cannot assess whether the counterintelligence goal set by the issued warrant has been achieved and cannot terminate the special measure prematurely.

An additional challenge is the practice of producing public information by both the SSSG and the Supreme Court of Georgia. These institutions typically refuse to provide statistical data, always citing the secret nature of counterintelligence activities. Without assessing the harm caused by disclosure, the blanket secrecy of data classified as public information is unacceptable.

The study of legislation shows that both the institutional setup and the existence of democratic control mechanisms are problematic. These mechanisms, under

the conditions of the secret nature of counterintelligence activities, would prevent human rights violations under the pretext of security arguments. Moreover, improving such mechanisms would restrain the excessive power held by the security sector and subject it to established standards of accountability and transparency.

Conclusion

The study aimed to assess the democracy and effectiveness of judicial oversight of surveillance mechanisms used by the security sector in Georgia. The first part of the study reviewed the main standards for the democratic use of surveillance mechanisms by the security sector, based on academic literature and international recommendations. The second part analyzed Georgian legislation and its practical enforcement, considering the peculiarities of the two regimes of using surveillance mechanisms: investigative (law enforcement) and counterintelligence (non-law enforcement). The study revealed that judicial oversight of the use of surveillance mechanisms is superficial and fragmented. Specifically, the following systemic problems were identified:

- Judicial oversight of the use of covert investigative actions only extends to the initial phase, i.e., the issuance of orders. The legislation does not provide mechanisms for proactive verification of actions during their implementation.
- The court does not verify whether the prosecutor's office fulfills its obligation to notify citizens about covert investigative actions after they are completed. The absence of such oversight mechanisms is particularly problematic given that the 2022 legislative reform significantly increased both the duration of the use of covert investigative actions and the postponement of notifications about them.
- The Personal Data Protection Service can only control the use of covert investigative actions through an electronic system if they are exclusively carried out by the Operational-Technical Agency. Other covert investigative actions (such as covert video or audio recording, photography, and electronic surveillance using technical means), which can also be performed by investigators, are not subject to direct technical oversight.

- The institutional subordination of the Operational-Technical Agency to the State Security Service (SSSG) creates a risk that the SSSG, which simultaneously performs counterintelligence and investigative functions, will abuse its authority and create “alternative banks” of surveillance outside the law through the Operational-Technical Agency. This risk is particularly high considering that the real mechanisms for ensuring the legality of personal data processing by the Personal Data Protection Service are quite limited, and it cannot fully control the activities of the Operational-Technical Agency.
- When issuing orders related to the use of covert investigative actions, the court is likely to rely excessively on the information provided by the prosecutor and does not critically and independently assess the necessity of using covert investigative actions.
- Counterintelligence activities are largely regulated at the level of subordinate normative acts, including the list of special services and operational measures that carry out counterintelligence activities is defined by orders.
- Some special measures defined by legislation are so vague that it is impossible to determine their content. It is impossible to assess the extent to which such measures interfere with basic human rights and freedoms.
- The legislation places only electronic surveillance and postal correspondence control measures under judicial oversight, leaving a range of special measures outside of democratic oversight.
- Statistics on electronic surveillance orders issued within the framework of counterintelligence activities are inconsistently or not at all maintained by the SSSG and the Supreme Court of Georgia.
- Judicial oversight of the use of covert investigative actions is non-transparent, and the public is not sufficiently informed about the effectiveness of the oversight. Specifically, the methodology of the covert investigative actions registry maintained by the Supreme Court is unclear, the court collects statistical data only selectively and fragmentarily, and does not analyze trends related to their use.

Recommendations

The presented study once again highlights the systemic failure of democratic oversight in the security sector. Therefore, it is essential to fundamentally review the levers at the disposal of the SSSG and the legislation governing their use. The mechanisms for external supervision and control over surveillance measures need to be systematically strengthened. Regarding judicial oversight over the security sector, the existing institutional, legislative, and practical issues in this direction must also be fundamentally reviewed.

Institutional and Legislative Arrangement:

- In accordance with international standards and recommendations, judicial oversight should extend not only to the commencement of covert investigative actions but also to their ongoing and concluding stages.
- The Operational-Technical Agency, which exclusively carries out surveillance measures, should be fully institutionally and functionally independent from the SSSG and law enforcement agencies. Additionally, this institution should not have investigative or counterintelligence tasks and interests, which would significantly reduce the risks of arbitrary and unjustified use of surveillance measures.
- The supervisory function of the Personal Data Protection Service over surveillance measures should be strengthened. Specifically, the service should have the right to conduct unplanned visits to the Operational-Technical Agency and have unrestricted access to their infrastructure.
- The supervisory mandate of the Personal Data Protection Service should extend to surveillance measures within the framework of counterintelligence activities. Specifically, the service should monitor the compliance of the measures conducted within counterintelligence activities with the orders issued by the Supreme Court.
- The duration of the use of covert investigative actions should be substantially reduced, and the exceptional cases allowing for the extension of surveillance terms up to the statute of limitations of a crime should be abolished. One option could

be to return to the durations stipulated by the legislative changes of 2022, which allowed for a maximum of 6 months (180 days) for conducting covert investigative actions and excluded the possibility of indefinite extension.

- The period for notifying a citizen about the covert investigative action conducted against them should be significantly reduced. One option could be to return to the durations stipulated by the legislative changes of 2022, which allowed for a maximum of 36 months for postponing the notification and excluded the possibility of indefinite postponement.
- The procedure for notifying a citizen about surveillance conducted against them should be clearly outlined in the legislation. Specifically, the law should specify the form of the notification and the information to be provided to the citizen. The citizen should also be informed about their right to appeal the measure at the time of notification.
- The current 48-hour period for appealing covert investigative actions should be extended to allow citizens to prepare a more quality and substantiated complaint. Additionally, the notification should be informative (including the grounds for the surveillance and the type of information obtained as a result) so that the citizen can effectively challenge the legality and justification of the measure.
- The existing structure of the SSSG should be reviewed, and structural reforms should be implemented to minimize the duplication of competencies between departments. As a result of the reform, the same department of the SSSG should not simultaneously have counterintelligence and investigative functions.
- The grounds and procedure for transferring information obtained within the framework of counterintelligence activities to other agencies should be clearly defined by law to prevent the abuse of information exchange possibilities by agencies. An external control mechanism must exist for the information exchange process.
- Instead of sub-legal normative acts, the list of special services authorized to carry out counterintelligence activities should be defined at the legislative level to exclude the arbitrary assignment of this function to any service by the executive authority that does not naturally fall under its mandate.

- Instead of one, all or several judges of the Criminal Cases Chamber should be designated as supervising judges, who will review the petitions presented by special services and decide on the issuance of orders on a rotational basis. This would mitigate potential biases of judges toward the arguments of special services.
- The supervising judge should be appointed not unilaterally by the court Chairperson but by the decision of the Supreme Court Plenum, whose primary functions include making such significant personnel decisions within the Supreme Court (such as determining the composition of chambers, appointing 3 judges of the Constitutional Court, determining the composition of the Grand Chamber, etc.).
- The Supreme Court should have oversight over all measures used within counterintelligence activities that result in interference with fundamental human rights and freedoms.
- Since the grounds for counterintelligence activities may be abstract and general, the court should assess the adequacy of restricting a person's rights based on abstract security threats when issuing orders for measures that limit rights.
- The judge's role in terminating electronic surveillance measures should be strengthened. If an interim report from the special service confirms that the counterintelligence task defined by the judge's order has been accomplished, the judge should have the authority to terminate the measure without waiting for the decision of the special service head.
- Legislation should specify not only the minimum 90-day duration for special measures but also the maximum duration for the entire cycle. The maximum duration for a one-time extension of the order (up to 12 months) should be reduced, and simultaneously, it should be specified how many times the special service can extend the validity of the order (maximum duration for the entire cycle). Otherwise, under the current legislation, the order duration may be indefinitely extended until another ground for terminating the measure is established.
- The decision to issue a written notification about the implementation of electronic surveillance measures against a person should be made not by the head of the special service but by the supervising judge. Each time, the judge should assess whether the security argument presented by the special service outweighs the individual's right to be informed.

- With the involvement of experts and civil society, a mandatory training module should be created for acting judges of the common courts and judicial candidates, covering the legal, technological, and political aspects of surveillance measures, best practices, and international standards.

Access to Public Information:

- The Supreme Court of Georgia should prepare and publicly publish the methodology for maintaining the register of covert investigative actions.
- All raw data related to the use of covert investigative actions should be statistically processed. This includes covert investigative actions conducted against state-political officials, judges, and persons with immunity, which are currently classified without any justification. The Supreme Court should publish detailed and comprehensive statistical information that would allow the public to have a real understanding of the quantitative trends associated with the use of covert investigative actions.
- Along with other statistical data, it should be mandatory to publish information on how many citizens were informed about the surveillance conducted on them and how many of them appealed this measure, as well as the outcomes of these disputes.
- Analytical reports should be published based on the collected and processed statistical data, characterizing the trends in the use of covert investigative actions and judicial oversight over them.
- The Supreme Court and the SSSG should publicize complete statistics regarding the implementation of electronic surveillance measures for counterintelligence purposes. This includes not only the approval rates of permissions but also the number of individuals subjected to surveillance under a single order. Such an approach would provide the public with a general understanding of the scale of counterintelligence activities without compromising state interests or counterintelligence objectives.