TRANSPARENCY INTERNATIONAL GEORGIA

DCAF
a centre for security, development and the rule of law

ადამიანის უფლებების სწავლებისა და მონიტორინგის ცენტრი
EMC
Human Rights Education and Monitoring Center

OPEN SOCIETY GEORGIA FOUNDATION

REFORM OF THE SECURITY SERVICE IN GEORGIA

RESULTS AND CHALLENGES

TBILISI 2018

Heads of the Research: Lika Sajaia, Sopo Verdzeuli
Lead Researchers: Mariam Mkhatvari, Gigi Chikhladze
Research of the International Practice: Nazli Yildirim Schierkolk
Also contributed to the research: Tamar Tatanashvili, George Topouria

We would like to thank the The Geneva Centre for the Democratic Control of Armed Forces (DCAF) for their contribution to the international practice chapter of this report.

This report was prepared by the financial assistance of the Open Society Georgia Foundation. The views expressed in the report belong to Transparency International Georgia and the Human Rights Education and Monitoring Center (EMC) and do not reflect the opinions of the the Open Society Georgia Foundation.

INDEX

INTRODUCTION

In the framework of the MIA reforms in 2015, the State Security Agency separated from the MIA and established itself as a separate institution. The separation of the police and security agencies was an important institutional move towards removing the concentration of excess power within the agency. However, it was clear at that stage that the separation itself would not be sufficient to establish a balanced, accountable and democratic control mechanisms over the security sector. The newly-established agency, as a result of the 2015 reforms, was given a number of problematic powers. The current law gives a broad mandate to the agency, which includes fighting against transnational organized crime and prevention, identification and eradication of corruption. Moreover, the State Security Agency also has powers similar to that of law enforcement agencies, such as crime investigation and arrest.

A broad mandate and law enforcement powers, coupled with the absence of strong guarantees of oversight and lack of experience, creates a foundation for excess power and unchecked authority within the State Security Agency. This damages the human rights situation and system of democratic governance in the country. These very risks associated with the security sector are the cause of concern amongst international and local actors who systematically stress about the necessity of democratic governance and oversight in the State Security Service.

This report is the first comprehensive document that assesses the institutional and legislative environment of the State Security Service in the aftermath of the 2015 reforms. The report also analyzes data on the activities of the last years of the State Security Service.

The aim of the report is to deliver a critical analysis of the institutional independence, mandate, oversight and accountability, as well as the quality of transparency, of the State Security Agency. Taking best practice, the legislative framework and issues related to the implementation of the law into account, the research also aims to single our challenges and recommendations based on the findings, as well to support subsequent reforms within the security sector.

The research project team would like to thank the Parliament of Georgia and the State Security Agency for collaborating in the research and providing us with public information. We would also like to thank the research and non-governmental organizations, as well as experts, for sharing their experience with us. A particular extension of gratitude goes to the Geneva Centre for the Democratic Control of Armed Forces (DCAF) for their contribution to the research on international best practice.

METHODOLOGY

The research covers the time period from the creation of the State Security Service on August 1, 2015, to December 31, 2017. The research uses retrospective analysis of the legislative framework. In this regard, the report analyzed the amendments made to the legislation that are related to the reforms on the institutional standing, functions, mandate and oversight of the security sector. The report is also based on the assessment of the implementation of the current law and the analysis of the information and individual interview data obtained from the State Security Service and its oversight bodies. The report also analyzed the standards of security sector set by the Council of Europe, United Nations, Venice Commission and other international organizations, as well as the experience of countries who are considered as hallmarks for best international practice.

The international standards of each chapter is accompanied by relevant overview of the practice of four countries. For the purposes of this report, and with the euro-Atlantic perspectives of Georgia taken into account, the following four countries have been selected:

- Germany and Belgium – Two European countries with a well-developed oversight and accountability systems, which are frequently brought up as examples of best practice in various reports and research of international organizations.
- Croatia – A European country with a recent history of democratization, which has carried out a significant reform within its security sector following its integration into the European Union
- Canada – A non-European country that is a member of NATO and OSCE, which is frequently brought up as example of best practice in various reports and research of international organizations.

It should be noted that there is no universally-acclaimed system for the governance and oversight over the Security Service and State Intelligence. Due to a unique setting for each country and an ever-changing global security environment, each country seeks to maintain a balance between security and human rights interests. The analysis of practice of four select countries in this report does not aim to outline only one path forward for Georgia in meeting its challenges in the security sector. Rather, the analysis of practice outlines differing approaches that have allowed for the establishment of institutional frameworks in line with international standards. These experiences, coupled with Georgian context and experiences, may be used as a springboard to incentivize discussions and finding the best solutions.

NOTE ON TERMINOLOGY

SECURITY SERVICE

The EU Fundamental Rights Agency makes a basic conceptual distinction between intelligence and security services: intelligence services are agencies have a foreign mandate and focus on countering external threats, while security services tackle domestic threats. [1] International standards and practices outlined in this report cover predominantly security services, but makes references to intelligence services whenever necessary.

The international practice chapter of this report, the 'security service' refers to "state bodies, including both autonomous agencies and departments/units of other government departments or the armed forces, that have a mandate to collect, analyze and disseminate intelligence within the borders of their state in order to inform decisions by policy makers, military commanders, police investigators and border/customs agencies about threats to national security and other core national interests."[2]

OVERSIGHT

The term oversight is frequently used in this study, and it is therefore important that it is clearly defined from the outset. Oversight is a comprehensive term that refers to several processes including: ex-ante scrutiny, on-going monitoring, and ex-post review, as well as evaluation and investigation. Oversight of security services is undertaken by a number of external actors, including the judiciary, parliament, National Human Rights Institutions (NHRI) and ombuds institutions, National Preventive Mechanisms (NPM), audit institutions, specialized oversight bodies, media and NGOs. Oversight should be distinguished from control as the latter term implies the power to direct an organization's policies and activities. As such, control is typically associated with the executive branch of government.[3]

1 European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks, (hereinafter EU FRA, Surveillance by Intelligence Services)* (Luxembourg, 2015), p. 13, available from: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

2 Council of Europe (2015) Democratic and Effective Oversight of Security Services, p.18, available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770

3 Born and Geisler Mesevage, 'Introducing Intelligence Oversight' in Born and Wills (ed.) 'Overseeing Intelligence Services: A Toolkit' (DCAF, 2012) p.6.

FINDINGS

General assessment of the reforms of the State Security Service

- The split between the Ministry of Internal Affairs and the Security Service was an important step forward in the right direction;
- The reform hasn't created strong guarantees for democratic system, accountability and oversight;
- The State Security Service is a closed and non-transparent institution, therefore it is difficult to monitor how it uses its resources and capabilities;
- The existing competencies of the State Security Service are unreasonably broad, vague and incompatible with the Service, for example - carrying out criminal investigations (including crimes related to corruption);
- In spite of the fact that the split of the Security Service from the Minister of Internal Affairs was labelled as a first step of the reform, no fundamental reforms followed in the security sector. Therefore, it is important for new stages of reform to be on the agenda.

1. INDEPENDENT GUARANTEES FOR THE INDEPENDENCE OF THE SECURITY SERVICE

- The risks of politicization of the State Security Service are high. The legislation doesn't duly provide guarantee for its institutional independence.
- The rules of appointment and dismissal of the Head of the Service are not sufficient enough guarantees for the independence of the Service;
- The appointment and/or early termination of the Head of the Service can be carried out with the sole decision of the ruling party. This, in turn, increases the risk of politicization of the system.

2. MANDATE OF THE STATE SECURITY SERVICE

- As a result of the 2015 reforms, one powerful Ministry was broken down into two structures – with excess of powers, duplicated functions and high risks of abuse of power. The mandate and scope of authority of the State Security Service is not clearly defined in the legislation, which creates risks of abuse of power when coupled with the high secretive nature and weak control of the Service;
- Particularly problematic are the following instruments available to State Security Service: investigative function, including on corruption related crime, law enforcement and functions enabling use of force, possession of a temporary detention isolator, existing system for secret surveillance, and the so-called "ODR" institute.

3. OVERSIGHT OVER THE SYSTEM OF THE STATE SECURITY SERVICE

- The oversight conducted over the State Security Service is not complex and a number of actors, including the Parliament, special bodies, executive government, judiciary, as well as the civil society, are not effectively and sufficiently involved in this process;
- According to the legislation, the Parliament is the main oversight institution over the State Security Service. Nevertheless, the legislative framework, limited mandate and low level of access to information does not allow for effective oversight to occur;
- The Parliament does not have sufficiently strong instruments to exercise effective and complete control over the State Security Service;
- A whole number of spheres and related events are carried out the State Security Service without any oversight (for example, protection of personal data in the Service and secret audio-video recording for counter-intelligence purposes).

- The Public Defender doesn't fully use or is hindered to fully use the powers vested in him over the Service;
- From the day of the formation of the Service as a separate structure (in 2015), there was no audit held, therefore it is unknown how reasonably the Service makes use of the allocated budgetary funds.
- Judiciary control does not cover secret audio and video surveillance conducted by the Service for counter-intelligence purposes. The judiciary does not check the ongoing operations nor does it inspect the destruction process of the obtained information;
- Judiciary control does not cover arranged surveillance, which represents the same intensity of intrusion into private life as the regular electronic surveillance;
- There are no external control mechanisms on the protection of personal data of secret surveillance operations that are not covered by judiciary control, such as presentation of information to specialized parliamentary oversight council, personal data inspector, etc.;
- Internal control mechanisms of the State Security Service are weak. There are no effective mechanisms for citizens to address the General Inspection of the State Security Service;
- An address made to the General Inspection does not oblige the Head of the Service to begin disciplinary proceedings;
- A citizen's address to the General Inspection related to a breach of law cannot be appealed.

4. TRANSPARENCY OF THE SECURITY SERVICE SECTOR

- The part of the statute of the State Security Service, which should include only the description of its functions, is classified.
- Public information is not issued based on the global principles of national security and rights to information, for example on the issuing of statistical information;
- The State Security Service does not fulfill the obligation on the complete publication of public information release reports (so-called December 10 reports) that are defined by the General Administrative Code of Georgia;

CHAPTER 1. RETROSPECTIVE ANALYSIS OF EXPERIENCES – SECURITY SECTOR IN GEORGIA

The State Security Service has existed in several different forms. Throughout the history of independent Georgia, the security agency existed beyond both the Ministry of Internal Affairs and the Cabinet. Currently, it functions as a service beyond the government cabinet.

From 1995 to current day, in parallel with changes to the forms of state governance and arrival of new political groups to executive power, the institutional standing and forms of accountability of the services working on state security have changed.

According to the initial draft of the Constitution of Georgia, any type of merger between the State Security and the Police was prohibited.[4] In 1998, the Parliament adopted a Law on the State Security Service, according to which the Service was a special-purpose government body. Through the Order of the President of Georgia, the statute of the Ministry of State Security was approved, according to which the Ministry guaranteed the internal security of the state from threats originating from internal and foreign sources. The Ministry was headed by the Minister of State Security, who was appointed by the President with the consent of the Parliament. The Minister could be dismissed by the President.[5] As a member of the Government, the Minister of State Security could be dismissed from office through impeachment. The Parliament had the power to remove the Minister from office due to a violation of the Constitution, state treason or other criminal offense.[6]

The Ministry consisted of 14 structural units [7], territorial bodies[8] and subordinate units[9]. The parliamentary control over the Ministry was exercised through the parliamentary Defense and Security committee[10]. The officials of the Ministry were accountable to the President. [11] As for the judiciary control, according to the Law on State Security Service, "investigative and procedural activities limiting human rights and freedoms recognized by the Constitution of Georgia may be carried out on the basis of a reasonable court decision". [12]

As a result of the amendments to the Constitution in 2004, the Parliament removed the provision that prohibited the merger between the State Security and Police. On March 1, 2004, through the Order of the President of Georgia, the regime of accountability of the Ministry of State Security was changed – it became accountable toward the government and was obliged in fulfilling the tasks defined by the law, Premier-Minister or the Government.[13]

In December 2004, on the basis of a draft law prepared by the Ministry of Justice, the Ministry of State Security was merged with the Ministry of Internal Affairs. Through the Order of the President, the sub-legal acts, which regulated the Ministry of State Security, were annulled. According to the explanatory note of the draft law, the existence of an independent Ministry of Security that wasn't accountable towards the Government was a remnant of the Soviet system. Moreover, the explanatory note stated that there was a duplication of functions, as well as an irrational allocation of human and material resources.[14]

4 Constitution of Georgia (1995 version), Article 78

5 *Ibid. 11.*

6 Constitution of Georgia (1995 version), Article 64

7 Counter-intelligence Service, Military Counter-Intelligence Service, Constitutional Order Protection Service, Anti-Terrorist Center, Investigative Service, Operative-Technical Service, Security Officers Units, Administration of the Ministry, Personnel Unit, Industrial Unit, Expertise-Criminal Unit, Communications Unit, Internal Security Unit, Financial Unit.

8 Ministry of the Autonomous Republic of Abkhazia; Ministry of Security of the Autonomous Republic of Adjara; Tbilisi Unit; Regional Units; District Departments.

9 Scientific-Technical centre, Academy, Military-Medicine Division

10 Law on State Security Service, Article 18.

11 *Ibid, Article 19.*

12 *Ibid, Article 20.*

13 Order of the President of Georgia N°74, on the Approval of the Statute of the State Security Ministry, Chapter I

14 Letter N°13145/2-4 of the Cabinet of the Parliament of Georgia

Following the liquidation of the Ministry of Security, its functions were distributed across various departments of the Ministry of Internal Affairs. In December, the Law on State Security Service was amended and the Law on Public Security Service was defined. On the basis of the new wording of the law, the public security service covered the departments of the Ministry of Internal Affairs and other structural sub-units, as well as special-purpose institutions of executive authority subordinate to the Government, which ensure public security and fulfilling tasks defined by the law.[15] According to the law, the Ministry of Internal Affairs is accountable to the President of Georgia and the Government. The Government of Georgia approved the state program of the Public Security Service. As for the appointment and dismissal rules of the Ministry of Internal Affairs, the Minister was appointed by the Prime-Minister with the consent of the President, while the dismissal was possible by both the Prime-Minister and President. As a member of the cabinet, the Minister of Internal Affairs was subject to impeachment procedures.[16] The Statute of the Ministry of Internal Affairs defined the sphere of activity of the Ministry: protection of state security and public order, detection, suppression, investigation and analysis of crimes and other violations of law, aims and activities of foreign countries, organizations and persons targeted against the vital interests of the country, as well as ensuring protection of the State border.

As it was subsequently made clear, the merger of these ministries produced an unprecendently powerful structure – the Ministry of Internal Affairs became a power giant. Many incompatible powers turned out in the hands of one Ministry, the secretive nature of the Security Service spread to departments of the Ministry, and external control and oversight became much more difficult.

One of the directions presented by the political coalition Georgian Dream for the 2012 parliamentary elections was the separation of the State Security Service from the Ministry of Internal Affairs and formation of a new Service with a new structure and form.

By the end of 2014, through the initiative of the Prime-Minister, the State Security and Crisis Management Council was tasked with starting reforms within the Ministry of Internal Affairs. During the reform process, the Government presented a fragmented concept, which did not meet the requirements for carrying out full-scale reforms in the law enforcement system. The concept concerned only the separation of the Ministry of Internal Affairs and State Security Service and subsequent amendments. No significant amendments were made.[17]

In the summer of 2015, the State Security Service separated from the Ministry of Internal Affairs. This separation was a move in the right direction, nevertheless, it did not result in the depoliticization of the law enforcement system and guarantees of democratic accountability and oversight.[18] The State Security Service created in 2015 is still characterized by excessive power and incompatible competencies, high level of secrecy and weakness in democratic oversight mechanisms.

According to the Law of Georgia on the State Security Service, "before 1 September 2015 the State Security Service of Georgia was tasked to establish the Commission, which shall ensure registration and inventory of the property transferred by and/or received from the Ministry of Internal Affairs of Georgia (including immovable property, material and technical base and other property) and official documents (including appropriate archive materials and other documents) as provided for by the legislation of Georgia". According to information provided by the State Security Service, the aforementioned Commission was functional. The Commission had also allegedly prepared a final document on its activities, but the State Security Service refused to disclose this document to us, citing the classified status of information contained therein.[19]

After 2015, the Government stated in 2017 its initiative for significant reforms for the State Security Service. In November 2017, the amendments initiated by the Government envisaged the merger of the State Border

15 Law on Public Security, Article 1, December 24, 2004 version

16 Order of the President of Georgia N°614, on the Approval of the Statute of the Ministry of Internal Affairs

17 EMC's assessment of the reform process and reform concept of the Ministry of Internal Affairs
https://emc.org.ge/2015/05/05/emc-is-shefasebebi-shss-s-reformaze

18 See: TI Georgia's Assessment of the Ministry of Interior reform
http://www.transparency.ge/ge/blog/shinagan-sakmeta-saministros-reformis-shepaseba

19 State Security Service Letter N°SSG51702131256.

Service with the State Security Service. The preparation of the following amendment was carried out hastily, without the participation of relevant experts and consultations with the civil society sector. The draft law presented to the Parliament provided a number of vague provisions, which were a target of criticism from the civil society.[20] A united civil security service with a mandate for internal and external intelligence causes the concentration of excessive power in one institution. Without a clear legislative base and strong oversight mechanisms, there are risks that foreign intelligence operations (which as a rule not regulated as strictly) will be used in the context of national security (which as a rule are more strictly regulated).[21] Based on this criticism and arguments, the Government addressed[22] the legislature and retracted its draft law.[23] Due to this, during the preparation of this report, the structure and functions of the State Security Service were largely unchanged and they correspond to the 2015 amendments.

20 See: EMC's First Report on the Ongoing Reforms in the Security Sector https://emc.org.ge

21 Venice Commission, *Report on the Democratic Oversight of the Security Services,* 2007, § 94-97 http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx

22 Decree of the Government of Georgia on the Removal of the Government's Draft Bill from the Parliament of Georgia. https://info.parliament.ge/file/1/BillReviewContent/166231

23 See: Assessment of TI Georgia http://www.transparency.ge/ge/post/saertashoriso-gamchvirvaloba-sakartvelo-dadebitad-apasebs-mtavrobis-gadacqvetilebas-uari-tkvas

CHAPTER 2. STANDING AND INDEPENDENCE OF THE SECURITY SERVICE

The label 'security service' refers to state bodies, including both autonomous agencies and departments/ units of other government departments or the armed forces, that have a mandate to collect, analyze and disseminate intelligence within the borders of their state in order to inform decisions by policy makers, military commanders, police investigators and border/customs agencies about threats to national security and other core national interests.[24]

As a rule, security services are subordinate to the subdivision of the cabinet, Ministries, such as the Ministry of Internal Affairs and Ministry of Justice. However, there are cases when they are directly subordinate to the Prime-Minister, President or both (Croatia). In a sense, subordination to one person or Ministry creates the risk of use of the Security Service for personal/political purposes.

As of today, the State Security Service of Georgia is a system of special-purpose institutions of executive authority subordinate to the Government of Georgia, which ensures state security within its authority.[25] The Government of Georgia approves the statute of the State Security Service.[26]

Minimal information on the activities of the State Security Service is not accessible and its activities are largely classified. Therefore, there is a risk of the improper use of the resources of the Service. In spite of the fact that neutrality is one of the foundational principles of the Service, today it is still a topic for debate how the institutional guarantees in place protect the use of the Service against political opponents of the ruling party, active opposition-inclined groups and citizens. Moreover, it is unclear how the institutional guarantees guarantee that the Service isn't used for serving the interests of the government, maintaining its power and stability.

According to the best practice overview by the United Nations Organization (UN), states are responsible on the international level for the activities of their special bodies[27], agents and for the work of any privately-hired persons, regardless of where this activity is taking place and who is target of the internationally-recognized illegal act. Due to this, the executive government exercises general control and is responsible for the activities of the special services.[28] The exact role of relevant government structural units and the scope of their control varies from country to country.

On one hand, executive control over the activities of the State Security Service is important for it to perform correctly and effectively. On the other hand, this control poses risk of the abuse of power from the side of the executive government, such as the use of the Service for personal and private political purposes, or exercising political influence or pressure over the activities of the Service. The part on international standards address the issue of abuse of power from the executive government:

- ***Subordination/open door policy:*** The open door policy can be a protective mechanism against such risks, for example, the relationship of the Heads of the Service with other Ministries, which it is not subordinate to. For example, in Great Britain, the Heads of the Secret Service, secret intelligence agency and the main communication departments of the Government are all subordinate to the Ministers of Internal Affairs and Foreign Affairs. Nevertheless, they still have a direct link to the Prime-Minister.[29]
- ***Differentiation of oversight and managerial control:*** When the executive government exercises general oversight over the security services, it should not imply in this function the direct responsibility of managerial control over the special and intelligence operations. According to the Democratic Oversight of the Security Services report by the Venice Commission: It will be impossible for political leaders to act as a source of external control if they are too closely involved in day-to-day matters and the whole

24 Council of Europe, *Democratic and Effective Oversight of Security Services,* 2015, pg.18, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770

25 Law of Georgia on State Security Service,Article 2.

26 *Ibid, Article 2.*

27 UN Compilation of Good Practices, pg. 4.

28 UN Compilation of Good Practices, N° 14.

29 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, 2005, pg.70.

oversight scheme will be weakened. There is the danger also of politicizing the intelligence cycle, with the consequence that the analysis stage and the end-product will be less useful."[30] Therefore, to prevent the abuse of power and unjustified interference, the state legislature should very clearly spell out the functions of the respective Ministry (or responsible public bodies) and the Head of the Service.

- ***Transparency of Government Instructions:*** Another protection mechanism, for the purpose of avoiding the use of government instruction for political purposes, is the subordination of government instructions to external control. While it is perfectly understandable that, for the purposes of protection of confidential data, it may be necessary to close access to the information for the public, the access of an expert oversight group to this instructions can be a mechanism.[31]
- ***Prohibition of the use of security services for political purposes and against political opponents:*** As per UN guidance, it is considered good practice when '[N]ational law prohibits intelligence services from engaging in any political activities or from acting to promote or protect the interests of any particular political, religious, linguistic, ethnic, social or economic group'.[32] For instance, the UK's Security Service Act has an explicit stipulation that 'that the Service does not take any action to further the interests of any political party'.[33] Another good practice endorsed by the UN is that '[I]ntelligence services are prohibited from using their powers to target lawful political activity or other lawful manifestations of the rights to freedom of association, peaceful assembly and expression'.[34] Such a provision in the law would serve as a strong basis for political neutrality.

Institutional guarantees for its independence are a significant method of reducing the risks of politicization of the security service. This, in turn, largely depends on the structure of the security service, as well as on the rules of appointment and dismissal of the Head.

2.1 MODEL FOR APPOINTING THE HEAD OF THE SERVICE

According to the Law of Georgia on the State Security Service, "a legally capable citizen of Georgia with higher education who is at least 35 years old and who has at least two years of working experience in the law enforcement bodies and who knows the official language of Georgia, may be appointed as the Head of the Service. A citizen of Georgia, who is at the same time a citizen of a foreign country, may not hold the position of the Head of the Service."[35]

The law defines the rules of appointment of the Head of Service as following:[36]

- Not earlier than two months and not later than eight weeks before the expiration of the term of office of the Head of the Service, the Prime Minister of Georgia shall nominate to the Government of Georgia a candidate for Head of the Service for review;
- The Government of Georgia, within one week after the nomination of the candidate for Head of the Service by the Prime Minister of Georgia, shall review the candidate and adopt an ordinance on the nomination of the candidate to the Parliament of Georgia under procedures provided for by the regulations of the Government of Georgia;
- If the Government of Georgia fails to adopt an ordinance on the nomination of the candidate for Head of the Service to the Parliament of Georgia, the Prime Minister of Georgia shall repeatedly nominate the same or another candidate to the Government of Georgia within three calendar days, after which the Government of Georgia shall follow the procedures determined by the aforementioned paragraph;
- If the Government of Georgia repeatedly fails to adopt an ordinance on the nomination of the candidate for Head of the Service to the Parliament of Georgia, the Prime Minister presents the same or another candidate.

The same candidate may be nominated to the Government of Georgia only twice.

---

30 Venice Commission, *Democratic Oversight of the Security Services*, 2007, § 143.

31 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, 2005, p. 69, http://www.dcaf.ch/making-intelligence-accountable

32 UN Compilation of Good Practices, N° 11.

33 UK, Security Service act, 1989, Article 2 (2)p, https://www.legislation.gov.uk/ukpga/1989/5/section/2

34 UN Compilation of good practices, N° 12.

35 Law of Georgia on State Security Service, Article 7.

36 *Ibid.*

The Parliament of Georgia, within two weeks after the nomination of the candidate for Head of the Service by the Government of Georgia, shall review the candidate and appoint the Head of the Service by a majority of the members, by secret ballot, under procedures provided for by the Rules of Procedure of the Parliament;

- If the candidate for Head of the Service fails to obtain the appropriate number of votes, the Prime Minister of Georgia shall nominate the candidate for Head of the Service to the Government of Georgia within one week;
- If the Head of the Service still fails to be appointed, the procedures provided in the aforementioned paragraphs are repeated. The process shall continue until a Head of the Service is appointed.

The same candidate may be nominated to the Parliament of Georgia only twice.

In spite of the fact that the appointment of the Head of the Service goes beyond the competencies of one branch of government[37] and includes the Parliament, the existing rule does not ensure that the appointment of the Head of the Service is not guided by narrow party interests. Given that the Prime-Minister, Members of the Government and the Parliamentary Majority belong, as a rule, to the same political group, the existing rules for appointing the Head of the Service do not tackle the risks of one political group single-handedly making the decision for the appointment of the Head. Due to the Prime-Minister's ability to single-handedly nominate the Head, there are grounds for the appointment to be political. The current rules for appoint of the Head does not recognize the participation of other political groups and is not orientated for reaching a consensus amongst political powers. Due to the Prime-Minister's ability to single-handedly nominate the Head, there are grounds for the appointment to be political. This is especially problematic when the qualifications required by law for the candidate are very broad.

Common practice shows that there is a dominant role of the executive government in nominating and appointing the Head of the Service. However, the standards are also important according to which there is a mechanism for democratic and inclusive consultation in the nomination process of the candidate. In this regard, there are varying practices across countries. In Australia, before the appointment of the Head, the Prime Minister has to consult with the leaders of the opposition parties.[38] In several European countries, including Estonia, Portugal, Hungary and Croatia, competent parliamentary committees carry out hearings with the candidate and they can issue non-binding opinions or recommendations. This type of involvement of the parliamentary committees (in most cases the committee that exercises oversight over the security services) provides the candidate with broad political support. Finally, in some country, such as United States of America and Romania, a plenary vote is held to support the candidate following the parliamentary committee hearings. It should be noted that while putting the candidate up for a vote before the Parliament is a democratic form, it still contains risks of politicization, such as turning into a party issue.[39] Moreover, in parliamentary models where the ruling coalition holds disproportionate number of parliamentary mandates (due to a minimal electoral threshold), the vote may fail to fulfill its purpose. In this case, obligatory consultations with the leaders of opposition and hearings in parliamentary committees can prove to be more effective.

2.2 SCOPE OF RESPONSIBILITY OF THE HEAD OF STATE SECURITY SERVICE

As already noted, the institutional independence of the Head of the State Security Service is connected not only to the rules of appointing employees, but their scope of responsibilities and their dismissal/suspension from work.

According to the existing law, the Head of the Service shall be accountable and responsible to the Parliament of Georgia. The Head of the Service, as the Head of the system of special-purpose institutions of executive authority directly subordinate to the Government of Georgia, shall also be accountable to the Government of Georgia.

37 Note: The Prime-Minister of Georgia presents the candidate to the Government, then the Government presents to the Parliament, and then the Parliament elects the Head of the Service by full-list majority.

38 Australia, Security Intelligence Organisation Act, Article 17(3),

39 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 2011, pg.107, 108

The law defines the grounds for the early termination of the term of office of the Head of Service,[40] and we can single out the grounds for the early termination,[41] for instances where the assessment of the work of the Head of Service is not required. One week after it has revealed or has been provided with information on such an instance, the Parliamentary Procedural Issues and Rules Committee will analyze the authenticity of the case and present a respective report at the nearest plenary session. The Parliament accepts the statement as a notification, which is written down in the protocol of the plenary sitting. Once the statement has been accepted as notification, the term of office of the Head of Service is terminated. [42]

In circumstances when the Head of Service fails to perform his/her duties for two consecutive months, took or holds a position incompatible with the office of the Head of the Service or conducts activities incompatible with his/her office, the Government of Georgia is authorized to issue an ordinance on the suspension of the term of office of the Head of the Service and on the submission of a request for early termination of the term of office of the Head of the Service to the Parliament of Georgia. The ordinance is immediately submitted to the Parliament of Georgia and the latter, within two weeks after its receipt, shall review and decide the issue of early termination of the term of office[43] of the Head of the Service by a majority of the total number of members, under procedures provided for by the Rules of Procedure of the Parliament of Georgia. If the Parliament fails to make a decision on early termination of the term of office of the Head of the Service, the ordinance of the Government of Georgia on the suspension of the term of office of the Head of the Service shall be annulled. [44]

In circumstances when the Head of Service fails to perform his/her duties for two consecutive months or holds a position incompatible with the office of the Head of the Service or conducts activities incompatible with his/her office, the Parliament of Georgia shall be authorized to review the matter of early termination of the term of office of the Head of the Service upon its initiative and under procedures defined in the Rules of Procedure of the Parliament of Georgia[45] and to make a decision for early termination of the term of office of the Head of the Service by a majority of the total number of its members.[46]

According to the law,[47] after hearing the report of the Head of the Service, at least one third of the members of the Parliament of Georgia on the current nominal list shall have the right to raise the issue of the dismissal of the Head of the Service, if during the hearing of the report, the necessity of making such decision arises. In this case the initiators shall specify reasons and/or grounds for raising such issue. The Parliament of Georgia shall make a decision to dismiss the Head of the Service by a majority of the total number of its members.

With all the aforementioned circumstances, it is clear that the Parliamentary Majority and the Government (which in our case is one single political group) hold the ability to singlehandedly dismiss the Head of Service. This significantly increases risks of politicization of these processes.

It is noteworthy that the aforementioned procedures for dismissal are different from the classical impeachment process. [48] The grounds for dismissal from office are not legally analyzed nor assessed by an independent body, which equals political responsibility. This, in turn, has an effect on the nature of the service and increases the risk of politicization.

---

40 Law of Georgia on State Security Service, Article 10.

41 Termination of Georgian citizenship; a judgement of conviction of a court against him/her enters into legal force; a court has declared him/her missing, dead or a beneficiary of support; he/she resigns voluntarily; he/she dies.

42 Rules of Procedure of the Parliament of Georgia, Article 229[6].

43 Law of Georgia on State Security Service, Article 10.

44 *Ibid.*

45 According to the Rules of Procedure of the Parliament of Georgia, the Parliament has the right, upon the conclusions of the Defense and Security Committee, and no longer than two weeks after the presentation of these conclusions, to consider the early termination of the term of office of the Head of the State Security Service. The decision is made with a closed vote by the majority of the votes of its acting members. If the voting is not held within the two week period and the last day of that period coincides with a day when there is no plenary session, then the voting will occur on the next plenary session. If the voting is still not held, then the voting is removed from the agenda.

46 Article 10 of the Law of Georgia on the State Security Service

47 *Ibid.*

48 The special process by which charges are levelled against a high official of government, the end result of which is the removal from office.

2.3 BEST PRACTICE OF SELECT COUNTRIES

Country	Subordination	Transparency of the Government Directives	Disclosure of information	Appointment and dismissal of the Head of the Service
Germany	• The BfV is subordinated to the Ministry of Interior • The BND reports to the Federal Chancellery	The BfV and BND is obliged to proactively inform the parliamentary oversight committee on the 'internal administrative directions/ developments with substantial ramifications for the pursuit of the services' mandate.	• Officials should first raise the issue of disclosure of information they are concerned with internally, within the service; • Afterwards, the issue can be shared with the committee;	The heads are appointed by the executive government.
Canada	The Canadian Security Intelligence Service (CSIS) reports to the Ministry of Public Safety and Emergency Preparedness.	A copy of each written direction issued by the Minister to the CSIS, should be submitted to the Security Intelligence Review Committee	The law outlines specific procedures for the officers of the CSIS to disclose information in the public interest. However, before disclosing the information, the officer should bring the matter to the attention of Deputy Attorney General, and in case of no response, with the Security Intelligence Review Committee, before disclosing the information	• The director is appointed by the cabinet, for a five-year term, renewable only once. The appointment process is open to all Canadians, transparent and merit-based.

Croatia	The Croatian Security and Intelligence Agency (SOA) is subordinated to both the President and the Prime Minister through the National Security Council	Regulations passed by the Government concerning the security service is classified and there is no obligation to proactively share them with oversight bodies, as is the case in Canada	• There are no mechanisms for disclosing information on wrongdoing in the interest of the public. Only in the circumstances when an officer receives an unlawful order from superiors, which constitute a criminal act, the person is obliged to notify the chairperson of the Parliamentary Committee and the head of the Office of the National Security Council	• The Director of the SOA is appointed by a decision co-signed by the President and the PM, for a four-year term, with possibility for renewal. • The law envisages the adoption of conclusions by the parliamentary committee on the internal policy and national security. • Before a final decision about the dismissal is reached, the opinion of the Croatian parliament may be sought
Belgium	According to the Organic Act on Intelligence and Security Services, The 'State Security', the civilian intelligence service of Belgium, is primarily subordinated to the Ministry of Justice, although the Ministry of Interior has also authority over the service insofar as it relates to maintaining public order and the protection of people.	• The National Security Council, which has been put in charge of inter alia, establish policies and priorities of the security service. Beyond the legal stipulation that the security service should carry out its activities in accordance with the directives set by the NSC, the Service is not, however, controlled by the NSC.	The members of the security service have the opportunity to disclose information to the expert oversight body. Complaints may be lodged without having to request authorization from superiors.	• The Director of the service is appointed by the King, de jure on the proposal of the Minister of Justice, but in practice by the government as a whole. The tenure term is five years and renewable. The Director is obliged to take the oath before the chairman of the Monitoring Committee for Supervision of the Intelligence and Security Services before taking office.

2.4 SUMMARY AND RECOMMENDATIONS

The independence and political neutrality of the State Security Service created in 2015 needs to be strengthened on the legislative level. This is directly connected to rules of appointment and dismissal of the Head of the Service.

Taken into account the fact that the appointment or early dismissal of the Head of the Service is possible through the sole decision of the ruling party, there are still high risks of politicization of the system. Bearing in mind the international standards and the experiences of the countries presented in the previous chapters, it is important to:

- For the purposes of strengthening the coordination between the Security Service and other law enforcement agencies, as well as for the prevention of direct political control and influence over the Service, the monitoring over the activities of the Service, as well as the planning of its activities, should be carried out jointly by various branches of the government and the coordination council that is created with the participation of the leadership;
- Strong guarantees of independence and political neutrality of the Service should be defined on the legislative level. In spite of the fact that the government exercises control over the Security Service, its scope should not include defense and intelligence operations. Due to this, the scope of authority of the executive government and the Head of the Service should be clearly differentiated on the legislative level. Moreover, the powers and responsibilities of the Head of the Service and other officials should be clearly defined on the legislative level. This is necessary so that the functions of the Head of the Service and other operative departments of the Service are clearly differentiated from each other;
- Government directives made towards the Security Service should be subject to external, parliamentary oversight. According to international best practice, a procedure should be worked out which will envisage the proactive sharing of any written directives with oversight bodies;[49]
- The role of the legislature should be strengthened in the process of appointment of the Head of Service and the parliamentary minority should be more engaged. Namely, there should be obligatory consultations with the parliamentary opposition in regards to the candidates for the Head of Service, as well as the hearing of the nominated candidates in relevant committees that exercise oversight over the Service. The committee exercising oversight over the Service should publish findings on the nominated candidates. The findings should be adopted by the Parliament prior to the vote on the candidates;
- The process of dismissal of the Head of Service should be carried out under the same rules as impeachment procedures;
- As per UN standards, it is good practice for national law to outline specific procedures for members of intelligence services to disclose concerns about wrongdoing. Accordingly, members of services should be protected from legal reprisals.50 However, for the purposes of preventing the abuse of making information public and protection of classified information, the legislation should clearly spell out the foundations and mechanisms for making information public. As per international best practice, the parliamentary oversight body should provide a platform, where the staff of the Service will be able to make public information related to crime, abuse of power by the management and undue interference.

49 See: Canadian Security Intelligence Service Act Article 6(2).

50 UN Compilation of Good Practices, N° 18.

CHAPTER 3. MANDATE OF THE SECURITY SERVICE

The definition of the structure, mandate and functions of the State Security Service have a significant impact on its functionability and its ability to protect fundamental rights and freedoms in a democratic society.

As per the 'UN Compilation Of Good Practices on Legal and Institutional Frameworks and Measures That Ensure Respect For Human Rights by Intelligence Agencies while Countering Terrorism' (hereinafter UN Compilation of Good Practices), the main purpose of security services is to '[*c]ollect, analyze and disseminate information* that assists policymakers and other public entities in taking measures to protect national security' and that '[M]andates are strictly limited to *protecting legitimate national security interests* as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address'.[51]

In this respect, the way national security threats are defined has a significant impact on the scope of the security services' mandates. The definition of national security and identification of respective threats is undeniably a national process, which should take into account the unique geopolitical and security circumstances of the country. Hence, there cannot be a strictly uniform list of threats to national security at the international level. However, case law of the European Court of Human Rights as well as the Parliamentary Assembly of the Council of Europe (PACE) recommendations provide guidance as to what is, and is not, commonly regarded as a threat to national security.

Born and Leigh compiled the following list of activities that are commonly considered as threats to national security based on the ECtHR case law: [52]

- Espionage (in Klass and others v. Federal Republic of Germany) [53]
- Terrorism (idem) [54]
- Incitement to/approval of terrorism (in Zana v. Turkey) [55]
- Subversion of parliamentary democracy (Leander v. Sweden) [56]
- Separatist extremist organizations which threaten the unity or security of the State (United Communist Party of Turkey and Others v. Turkey) [57]

It should be noted that this list is not exhaustive, and other matters such as interference with electronic data relating to defense, foreign affairs or other matters affecting the vital interests of the State may also be considered as a threat to national security.[58]

The forthcoming sub-chapters provide an overview of the mandate of the State Security Service, specific problematic powers and respective international standards.

51 UN Compilation of Good Practices, N°2.

52 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, 2005, pg. 30

53 See: http://hudoc.echr.coe.int/eng?i=001-57510 § 48

54 *Ibid.*

55 See: http://hudoc.echr.coe.int/eng?i=001-58115, § 49-50

56 See: http://hudoc.echr.coe.int/eng?i=001-57519 § 59

57 See: http://hudoc.echr.coe.int/eng?i=001-58128 § 39-41.

58 Council of Europe, Experts Report: European Committee on Crime Problems (CDPC), Group of Specialists on Internal Security Services (PC-S-SEC), Addendum IV, Final Activity Report, 40703, § 3.2.

3.1 INVESTIGATIVE FUNCTION

During the process of formation of the State Security Service in 2015, the civil society has criticized giving investigatory functions to the Service[59]. The Government of Georgia did not these recommendations into account. Under the existing legislation, the State Security Service has the power to eliminate (carry out preventive measures), identify, prevent and investigate crimes falling within the investigative jurisdiction of the Service. Mandating the Service with investigative powers is incompatible with the analytical-counter-intelligence activities of the Service. Moreover, excessive power is concentrated within the Service under the conditions when there is no control over the sharing of information, which are obtained through investigative operations, between law enforcement bodies.

According to the Law of Georgia on the State Security Service, the authority of the Service includes the analysis of crimes falling within investigative jurisdiction of the Service. As per the same law, the areas of activities of the Service for ensuring state security include the following: [60]

1. Protecting constitutional order, sovereignty, territorial integrity and military capabilities of Georgia from unlawful acts of foreign special services and individuals;

2. Identifying unconstitutional and forceful changes of the constitutional order and state government of Georgia and ensuring the protection thereof

3. Ensuring economic security of the country;

4. Combating terrorism;

5. Combating transnational organized crime and international crime threatening the state security;

6. Carrying out measures for preventing, identifying and eliminating corruption;

7. Protecting state secrets and carrying out measures to ensure the protection of state secrets under procedures provided for by the legislation of Georgia and ensuring the monitoring of the implementation of such measures;

8. Protecting the country from external threats.

The Order of Ministry of Justice defines the mandate of the criminal law and territorial cases, according to which the mandate of the State Security Service, in addition to other crimes, covers violation of human equality (Article 142 of the Criminal Code of Georgia), which implies the violation of human equality on the grounds of language, sex, age, nationality, origin, birthplace, place of residence, material or rank status, religion or belief, social belonging, profession, marital status, health status, sexual orientation, gender identity and expression, political or other views or of any other signs that have substantially breached human rights.[61] From August 1, 2015 until November 2017, there were no criminal cases launched or terminated under this article. According to information provided by the State Security Service[62], within the same time period, the Service had one case pending under the aforementioned article, which was transferred to it from the Prosecutor's Office of Georgia. The case was closed due to lack of any criminal breaches. It is unclear and vague why a special law enforcement such as the State Security Service should have the mandate to prevent/investigative violation of human equality. Naturally, this mandate may allow the Service to have specific groups and regions under active surveillance. Statistical data doesn't exclude active operative/pre-investigative operations conducted under the pretext of preventing crimes related to violation of human equality. The vague wording of the provision itself contributes to raising the risks of abuse of power and massive surveillance.

We contacted the State Security Service and requested information structural sub-units, which have the right to conduct criminal investigations under procedures determined by the Criminal Procedure Code of Georgia. According to the Service, the competencies and powers of the respective structural sub-units is defined by the Law of Georgia on State Security Service, Statute of the State Security Service and Statutes

59 See: The Coaliation's Assessment of the Independent and Transparent Judiciary: http://coalition.ge/files/comments_on_the_ministry_of_internal_affairs_reform_concept_25092015_ge.pdf

60 Law of Georgia on State Security Service, Article 5.

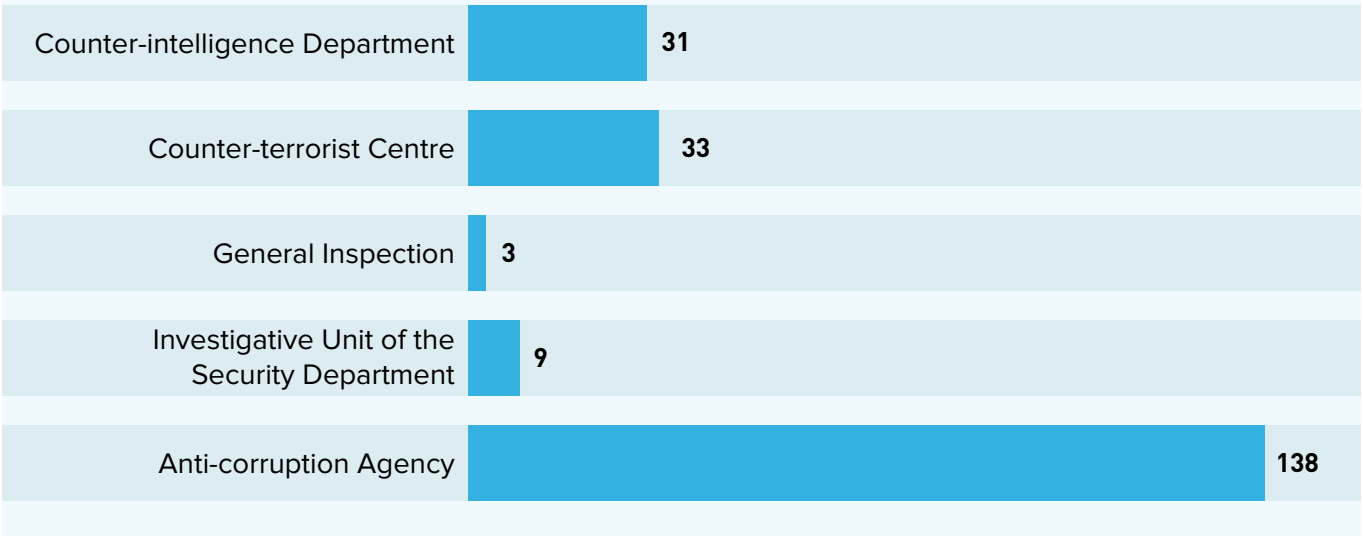
61 Chief Prosecutor's Office Letter N°13/82189.

62 State Security Service Letter N°71702929309.

of individual sub-units, most of which are classified. Therefore, according to the response of the Service, the issuing of additional information is prohibited by the Law of Georgia on State Secrets.[63]

According to the Statute of the State Security Service, investigatory activities are carried out under procedures determined by the Criminal Procedure Code of Georgia by the General Inspectorate of the State Security Service[64], Counter-Intelligence Department[65], State Security Department[66], Anti-Corruption Agency[67], Counter-Terrorism Center[68], in cases provided by the Prosecutor General of Georgia or an authorized person.

INVESTIGATIONS STARTED IN STATE SECURITY SERVICE ON CRIMINAL CASES (AUGUST 1, 2015 - DECEMBER 2017)



It is problematic that the main area of activity of the Service is carrying out measures for preventing, identifying and eliminating corruption. This type of crime, along with other types of crimes, should be investigated by the Service only when it poses a direct and immediate threat to the security of the State. In other cases, the power of the Service can be interpreted as a concealed mechanism of control over the civil service.

According to PACE Recommendation 1402, internal security services should not be authorized to carry out law-enforcement tasks such as criminal investigations, arrests, or detention. Due to the high risk of abuse of these powers, and to avoid duplication of traditional police activities, such powers should be exclusive to other law-enforcement agencies.[69] Similarly the UN Compilation of Good Practices acknowledges the strong arguments made against combining intelligence and law enforcement powers in one agency, taking into consideration the risk of developing a parallel enforcement system.[70]

In line with these international standards, most democratic states limit the mandate of their security services to collection, processing and dissemination of information; and do not entrust them with law enforcement powers.

The Parliamentary Assembly of the Council of Europe, in its landmark Recommendation 1402 (1999) on 'Control of internal security services in council of Europe member states' stated that '[E]conomic objectives,

63 State Security Service Letter N°21702134151.
64 Statute of the State Security Service, Article 7.
65 *Ibid.*
66 *Ibid.*
67 *Ibid.*
68 *Ibid.*
69 PACE Recommendation 1402, Guideline B3.
70 UN Compilation of Good Practices, § 41.

or the fight against organized crime per se, should not be extended to the internal security services. They should only deal with economic objectives or organized crime when they present a clear and present danger to national security'.[71]

This statement is open to interpretation as there is no objective measure of what types of economic/ organized crime present clear danger to national security. By way of example, in a recent judgment, (C.G and others v. Bulgaria) the ECtHR ruled that 'drug trafficking' in the context of the case concerned, cannot be considered as a threat to national security.[72]

In line with those normative standards and case law, many states do not entrust their security services with a mandate to counter organized crime and other crimes with economic gains such as corruption. Amongst the advanced European democracies such as Germany and the UK, combatting organized crime and corruption falls within the mandate of police or specific law enforcement units/agencies, and not the security services.

However, some states include 'protection of vital economic interests' in the definition of national security. If the 'vital economic interests' are not well defined in the law, there may be a risk of misuse of the mandate of security services. In this respect, the Venice Commission states that proliferation of weapons of mass destruction, circumvention of UN/EU sanctions, and major money laundering are three areas that could be legitimately included in the mandate.[73]

3.2 LAW ENFORCEMENT AND USE OF POWER

One of the functions of the State Security Service is to carry out preventive measures in order to prevent threats to state security . [74]

According to Article 13 of the Law of Georgia on State Security Service, if there are reasonable grounds to believe that state security may be at risk, the Service shall take the following preventive measures within its scope of authority:

- questioning a person;
- identifying a person;
- summoning a person;
- carrying out frisk and examination of a person;
- carrying out special frisk and examination of a person;
- ordering to leave a place and prohibiting entrance to a certain territory.

Notably, this list isn't exhaustive and that the Service may carry out other preventive measures without interfering with fundamental rights and freedoms of a person

Notably, the preventive measures of the Service are largely similar to the powers vested in the Police.[75] The legislation regulating the preventive measures of the State Security Service significantly expands the ability to interfere in the freedom and private life of persons on the grounds of protecting state security. The high level of interference in rights and freedoms of a person are further exacerbated by the fact that the grounds for conducting preventive measures are broad, and as a rule, are directed towards abstract threats.

71 PACE Recommendation N° 1402, Guidelines N°A2
http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en

72 see: http://hudoc.echr.coe.int/eng?i=001-86093, § 40-43

73 Venice Commission, *Report on the Democratic Oversight of Signals Intelligence Agencies*, 2015, pg.20
http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)011-e

74 Law of Georgia on State Security Service, Article 12.

75 Law on the Police of Georgia, Article 18.

The analysis of the grounds of conducting preventive measures also raises another issue. A preventive measure is significantly different from other types of mechanisms (investigatory mechanisms) due to the level of protection of rights of a person, as well as due to the different nature of oversight by the Prosecutor's Office and judiciary. As already noted, the use of preventive measures is also allowed in cases when information is available on the crime committed. This formulation points to the legislator's will to give the State Security Service the ability to carry out preventive measures on a crime already committed. This, in turn, results in less oversight over the activities of the Service and less guarantees of protection for citizens.

The exercise of preventive powers is problematic[76] even for the officials of the Ministry of Internal Affairs, which specifically prepare for such activities beforehand and at most times wearing uniforms and shoulder cameras. The scope of the problems associated with preventive operations increases in the case of the State Security Service, which isn't structured for such contact with citizens.

According to the Law of Georgian on State Security Service, authorized divisions and employees of the Service may use coercive measures, including the use of physical force, special equipment and firearms. [77]

The rules for the keep and use of special equipment is defined in more detail in the Order of the Head of the State Security Service. According to the sub-legal act, the rule envisages the ability of the employee to fulfil their work in preventing crime, detaining a criminal, ensuring state security and fulfilling other legitimate objectives of the State Security Service. [78]

The legislative framework defines active and passive special measures. Passive special means include: bulletproof vests, helmets, riot shields, gas masks and other special body protective equipment, while active special means include: handcuffs and other means of restraint, rubber batons, tear gas, pepper spray, sonic weapons, non-lethal weapons (including non-lethal shells), flash-bang device of psychological effect, a device to stop a vehicle by force, barrier demolition equipment, water cannons, an armored car and other special vehicles, special paint, service dogs and horses, electroshock devices and a capturing net.[79]

The Order of the Head of the State Security Service defines the powers of use of the special measures by the respective structural units of the Service.

Structural units of the Security Service	Special measures that can be used in special cases
A) Special-Operative Department, B) Counter-Terrorist Centre C) Protection of State Object Division D) Special Means Division of the State Security Service E) Temporary Detention Isolator Department	All passive and active special measures
A) Anti-Corruption Agency B) Counter-Intelligence Department C) Operative-investigative units of the State Security Department	Handcuffs, rubber batons, electroshock devices

Notably, the list of special means which can be used by the State Security Service is identical to the special means which can be used by the Ministry of Internal Affairs. [80] According to international best practice, the

76 *EMC*, Prevention of Crime emc.org.ge

77 Article 23 of the Law of Georgia on State Security Service

78 Article 1 of the N°2 Order of the Head of the State Security Service

79 *Ibid, Article 2.*

80 Law of Georgia on the Police, Article 33.

Security Service should provide information on potential risks retrieved from its analysis to law enforcement structures. Notably, the majority of democratic states do not give internal security services the right to use force. Even more so, the employees of the internal security services do not have more right to use force than regular citizens.

3.3 TEMPORARY DETENTION ISOLATOR DEPARTMENT OF THE STATE SECURITY SERVICE

In March 2017, as a result of amendments, two problematic powers were added to the State Security Service. Namely, confining an arrested person to a temporary detention isolator.[81] Comparatively more details on the norms regulating the temporary detention isolator were written in the Statute approved by the Head of the Service and in the Internal Rules of the Detention Isolator.

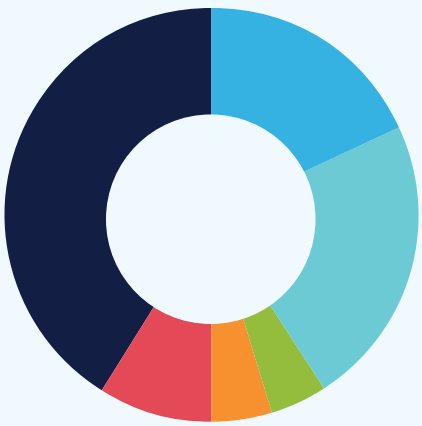
The basis for placing persons in the Isolator are as following: [82] a) detention report; b) detention report from the court; c) detention report of the defendant; d) verdict of the judge according to Article 205 (6) of the Criminal Code of Georgia[83].

Persons are placed in the isolator in cells, where there may be video surveillance and other forms of control as defined by the legislation, for the purposes of preserving the safety of the person and ensuring the protection of the requirements of the Internal Rules of the Isolator.[84]

Notably, the existence of a separate temporary detention isolator within the State Security Service is connected with several risks, including: harsh regime, different rules for security, low guarantees of protection of rights of the detainees, limitation of communication with lawyers, etc.

According to public information provided by the State Security Service, it is possible to accommodate a maximum of 21 persons in the temporary detention isolator N1 of the State Security Service.[85]

22 PERSONS HAVE BEEN CONFINED IN THE TEMPORARY DETENTION ISOLATOR OF THE STATE SECURITY SERVICE (TIME PERIOD: FROM THE ISOLATOR'S ESTABLISHMENT TO DECEMBER 2017)



9	Taking bribe
2	Comlicity in bribe taking
1	Giving bribe
1	Purchase, storing, carrying of fire-arms
5	Commercial bribery
4	Financing or providing resources to terrorism

81 Law of Georgia on State Security Service, Article 12.

82 Internal Rules of the Temporary Detention Isolator of the State Security Service of Georgia, Article 3.

83 Note: If the court is territorialy far away from the petentiary establishment and the transport of the defendant is difficult, through the Court's Decision it is possible to transport the defendant to the nearest petentiary establishment or temporary detention isolator. During this time, the Ministry of Corrections will be in charge of the defendant.

84 Internal Rules of the Temporary Detention Isolator of the State Security Service of Georgia, Article 4.

85 November 21, 2017 Letter of the State Security Service

According to UN Compilation of Good Practices: "Intelligence services are not permitted to operate their own detention facilities or to make use of any unacknowledged detention facilities operated by third parties.' This is an important safeguard against incommunicado detention[86], torture and other forms of ill-treatment[87].

3.4 EXISTING SYSTEM OF SECRET SURVEILLANCE

In 2016, the Public Defender and the "This Affects You Too" campaign filed a lawsuit in the Constitutional Court and demanded to recognize as unconstitutional the provisions of the Criminal Procedure Code and the Law on Electronic Communications, which gave the Security Service direct access to information and the storage of metadata for two years.

On April 14, 2016, the Constitutional Court of Georgia ruled the existing system of secret surveillance as unconstitutional.[88]

The Decision of the Constitutional Court reads: "The State Security Service possesses technical capabilities for eavesdropping and monitoring online communications, which allow collection of personal information in real time. While it is true that there is a presumption that the respective body won't abuse its powers, there are risks of unjustified intrusion into private life due to the ability to collect, store, and administer private information in real time, to copy and store metadata by agencies that have an investigative function or is professionally interested in obtaining this information."

For the purposes of drafting the legislative amendments, the Parliament created a working group in January 2017. The ruling party presented a draft law to the working group, according to which the right to conduct secret surveillance over telephone and internet communications, as well as secret video and audio recordings, were transferred to an LEPL subordinate to the State Security Service. [89]

In spite of criticism from the civil sector[90], the Georgian Parliament adopted with III hearing the Law on LEPL-Technical Agency on March 22, 2017. According to the law, the mandate of direct access to information and surveillance technical equipment will be given the Operative-Technical Agency of Georgia, which is an LEPL within the State Security Service. The Operative-Technical Agency provides support to all agencies that conduct secret surveillance operations. With the adoption of the new law, the rights of the department of the State Security Service was transferred to an LEPL subordinate to the same Service. Due to this, the Decision of the Constitutional Court was not upheld.

The nature and institutional structure of the new Agency is noteworthy. It is an LEPL subordinate to the State Security Service, and the institutional structure, formation rules, as well as functions, all point to it being a professionally interested agency, which still has direct access to telephone and internet communications, as well as collects and copies identification data.

The Head of the State Security Service plays a crucial role in the process of selecting the Head of the Agency. Namely, he presents a minimum of three nominees for the Head to a special commission. Notably, the special commission is shared by the Head of the State Security Service, who also has the right of vote.[91]

86 Incommunicado detention is generally understood as a situation of detention in which an individual is denied access to family members, or an attorney, or an independent physician. This approach frequently supports torture, which is high in the non-existence of public control. See: https://goo.gl/sXW5Ep

87 UN Compilation of Good Practices, Nº 30

88 April 14, 2016 Decision of the Constitutional Court of Georgia http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridze-tatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashoriso-gamchvirvaloba-saqartvelo-aaip-saqar.page

89 Campaign This Affects You about the Initiative on Secret Investigative Activities https://www.esshengexeba.ge/?menuid=9&lang=1&id=1147

90 Statement of the This Affects you Too Campaign: the new legislation regulating secret surveillance doesn't provide inviolability of private life and the Constitution of Georgia is still breached https://www.esshengexeba.ge/?menuid=9&lang=1&id=1151

91 Law of LEPL - Technical-Operative Agency of Georgia, Article 19.

Moreover, the Head of the Agency is obliged to seek the consent of the Head of the Service in such important institutional issues, such as:

1. Material-technical support and funding; [92]

2. Internal structure of the Agency, staff list and basic salaries of the employees of the Agency; [93]

3. The Head of the Service defines the general structure of the Agency and competencies of the structural sub-units and territorial divisions.[94]

Notably, beyond these competencies, the State Security Service is presented as one of the oversight institutions of the Agency.[95]

Therefore, the Agency cannot be considered as independent from the State Security Service.

As for the broad powers of the newly created Agency, it carries out not only the surveillance/recording of telephone conversations, but also secret investigations[96] and counter-intelligence activities. [97] The Agency's competencies also include the licensing, checking electronic communication companies and presenting them with obligatory technical requirements. Notably, these competencies also fall under the National Communications Commission.

The adoption of the aforementioned legislative package by the Parliament was assessed by the civil society as an unfortunate precedent for neglecting the decision of the Constitutional Court of Georgia. [98] The Agency retained the right to direct access to electronic communications, [99] while the broad competencies of the new Agency still provide it with the ability and interest to process big volumes of information, including personal data. Therefore, there are still risks for the State Security Service to abuse power.

Unfortunately, the aforementioned reform did not solve the problems related to the inviolability of private life in the country. In certain instances, the risks for violating the untouchability of private data was increased.

The Constitutional Court ruled on April 14, 2016 that the control mechanisms of the Personal Data Protection Inspector, such as the power to terminate or initiate surveillance of telephone conversations, were not sufficiently effective. In spite of the Constitutional Court's ruling, this oversight mechanism was further weakened during the reform. The Inspector can no longer issue a technical order over the initiation of surveillance of telephone conversation and it only has the right to terminate the surveillance.[100]

Prior to the reform, only one department (State Security Service Operative-Technical Department) had the right to conduct telephone conversation surveillance and recording. After the reform, the newly created Agency is also allowed to have territorial divisions, which points once again to the scope of power of the Service and the risks of illegal interference in private life.[101]

As it has already been noted, the newly created Agency does not carry out secret surveillance/wiretapping of electronic communications and thus does not provide assistance to law enforcement agencies in this regard; the Agency has also retained operative-investigative function. At the same time, the Agency has a new coercive measure against private companies, while on the other hand the legal standing of the private companies has worsened. Vesting such powers within the Agency with such powers once again poses risk to the inviolability of private life of citizens.[102]

92 Ibid, Article 20.
93 Ibid.
94 Ibid, Article 22.
95 *Ibid, Article 29.*
96 Law of LEPL - Technical-Operative Agency of Georgia, Article 8.
97 *Ibid.*
98 277 citizens addressed the Constitutional Court with a constituational case prepared by the This Affects You Too Campaign
99 *Ibid, Article 8.*
100 *Ibid, Article 2.*
101 *Ibid, Article 3.*
102 *Ibid, Article 8.*

As of today, the Constitutional Court of Georgia is deliberating on the lawsuit filed by 326 citizens, who are protesting LEPL-Operative-Technical Agency's technical capacity of secret surveillance to obtain real-time access to communications, as well as the powers of the Agency to copy and store electronic communication's metadata.[103]

3.5 "ODR" INSTITUTE

Prior to the reforms in the summer of 2015 and the separation between the Ministry of Internal Affairs and State Security Service, and according to the Statute of the Ministry of Internal Affairs in power at that time, the Minister of Internal Affairs of Georgia was authorized to appoint security officers (so-called ODRs) in other state institutions and important organizations. [104] According to the same Statute, the Counter-Intelligence Department [105] and State Security Agency [106] were responsible for the coordination and control of the security officers.

It should be noted that the malpractice of the so-called "ODR" has been a frequent target of criticism from the civil society sector.[107] In a sense, the "ODR" mechanism gave the State Security Service the legal right to exercise total control over the public and private institutions, to monitor the processes in the public sector, as well as exercise control over the political and public life. As a result of the reforms in 2015, the issues of security regime for entities posing a high risk to state security were defined by law, however there are still no oversight forms over their activities.

According to the transitional provisions of the new Law of Georgia on State Security Service, the Government of Georgia had to approve before 1 January 2016 the list of the institutions posing high risk to the state security. [108]

In order to ensure state security at entities posing a high risk to state security, Article 22 of the Law of Georgia on State Security Service, the Service has the right:

- to establish a security protection regime, under an ordinance of the Government of Georgia, for entities posing a high risk to state security, depending on their specifics, and provide them with appropriate consultations on matters related to the protection of state security;
- to create an effective system of exchanging information with entities posing a high risk to state security;
- to monitor the compliance with security protection regime at entities posing a high risk to state security, and give such entities appropriate instructions where threats posing a high risk to state security are identified;
- to conclude a cooperation agreement [109] with the entity posing a high risk to state security upon the written request thereof.

As for the list of entities posing a high risk to state security, the Resolution of the Government defines the following entities: Ministries of Georgia,[110] Government of the Autonomous Republic of Adjara, Batumi Municipality City Hall, Tbilisi Municipality City Hall, JSC Telasi, JSC Georgian Railways, JSC United Energy System Sakrusenergo, ltd. Enguri Dam, ltd. Sakaeronavigatsia, and others.

---

103 https://goo.gl/hPq6n6

104 Article 5 of the July 30, 2015 Statute of the MIA

105 *Ibid. Article 10.*

106 *Ibid.*

107 Coalition provides an opinion on the process of reform of the Ministry of Interior: http://coalition.ge/index.php?article_id=62&clang=0

108 Article 51 of the Law of Georgia on State Security Service

109 The agreement may include: Type and scope of cooperation between the Servie and high risk subjects, including the appointment of a representative of the Service for monitoring the protection regime; the issue of renumeration for carrying out the protection regime.

110 Ministry of Finance, Ministry of Healthcare and Social Affairs, Ministry of Economy and Sustainable Development, Ministry of Protection of Environmental Resources, Ministry of Corrections and Probation, Ministry of Foreign Affairs, Ministry of Regional Development and Infrastructure, Ministry of Agriculture.

The institution of the so-called "ODRs" became a topic for discussion in March 2016 during the protests at the Tbilisi State University. During the protests, there was numerous information that state security officers were working at the university. The Rector confirmed the existence of the so-called "ODRs" at the last meeting of the Academic Board. The Rector noted that the "ODRs" existed prior to his appointment and that the security officers changed during his tenure.[111]

The "ODR" institution infringes on the independence of institutions of government and interferes with the country's democratic development. Moreover, it can be used as a mechanism for protecting the ruling political regime. The actualization of this issue at the background of the student protests indicates that the "ODR" institution is the control of public attitudes and protection of the state from strong social protests.

Universities are not and cannot be included in the list of entities posing a high risk to state security approved by the Resolution of the Government. In spite of this, it is clear that the reforms carried out in the summer of 2015 were insufficient to address the issues at hand:

- In spite of the fact that the "ODR" institute was established anew, the legislation did not improve the issue of dismissal of security officers, who were employees of respective institutions and fulfilled administrative functions at the same time;
- The newly created State Security Service is an absolutely closed and non-transparent institution, which is practically not subject to any form of external control. Therefore, the public has no means to control over how the Service uses its resources and capabilities112

Non-governmental organizations addressed the Parliament with a request to set up a temporary investigative commission to look into the so-called "ODR" institute. [113] After the amendments to the law, the Public Defender also called on the Parliament to create a temporary investigative commission to look into the practice of the so-called "ODR" institute. [114]

We requested information from the State Security Service on the number of institutions from which security officers (ODRs) were recalled and the total number of security officers recalled. Unfortunately, the Service did not provide us with this information and notified us that the staff list of the Service does not even envisage the position of security officers.[115] For clarifying information, we requested additional information on the number of entities posing a high risk to national security and how many cooperation memorandums have been signed (with reference to the entities). Unfortunately, the information provided by the State Security Service is vague and incomplete. According to the Service, they have agreements with the entities that are approved and defined by the Decree of the Government. As for the security regime, according to the information provided by the Service, the document is classified and therefore they are unable to provide any additional information about it.

3.6 LEGAL STATUS OF FOREIGNERS AND FUNCTIONS OF THE STATE SECURITY SERVICE

The procedures defined by the legislation on refugees and sublegal acts on the denial for issuing/renewal of residence permits are vague and the risks associated with the State Security Service are most evident in the cases of the Azeri journalists, politicians and activists. Azeri citizens, during the period of their entrance and stay in Georgia, are denied in receiving documentation necessary for legal residence in Georgia without a reference to the reasoning behind such determination. The basis for the denial is mostly made in reference to national interests and public security, which is in turn based on the determination of the State Security Service.[116]

111 EMC responds to the alleged existence of ODRs in TSU: https://emc.org.ge/2016/03/09/emc-16/

112 NGOs address the Parliament for creating an investigative commission for the ODRs https://emc.org.ge/2016/03/21/emc-23

113 *Ibid.*

114 See: The sub-chapter of this report: The role of the public defender in the oversight over the State Security Service

115 State Security Service Letter N°SSG 21702134151.

116 see: *IPHR, Freedom now, EMC,* Repression Beyond Borders: exiled Azerbaijanis in Georgia https://emc.org.ge/2017/11/21/emcraport

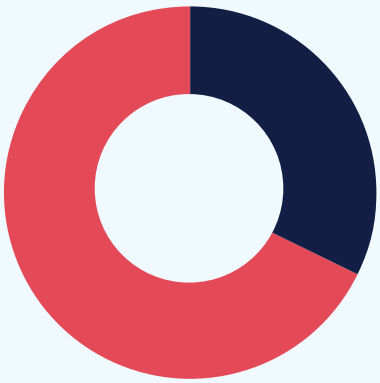
The procedures for granting refugee status is regulated by the Law of Georgia on International Protection, according to which: "Refugee status shall be granted to an alien or a stateless person, who is outside the country of origin, and has a well-grounded fear that he/she may become a victim of persecution on the grounds of his/her race, religion, nationality, affiliation to a certain social group or political views, and who does not wish to, or cannot, return to his/her country of origin or enjoy the right to be protected from such country due to such fear."[117] The decision to grant refugee status is made by the Ministry Of Internally Displaced Persons From The Occupied Territories, Accommodation and Refugees of Georgia. The refuge status may be denied if there are sufficient grounds to believe that he/she will endanger the state security of Georgia, its territorial integrity or public order. [118]

The Ministry addressed the State Security Service to determine the potential threat to national security[119]. The Service, in return, carries out the identification and verification of the data related to the refugee claimant. Moreover, the Service issues a recommendation to the Ministry on the potential threat that the refugee claimant may pose to the national security of Georgia.[120]

Azeri journalists and politicians are denied a refugee status in Georgia mostly on grounds of posing a threat to state security and territorial integrity.[121]

In one of the cases the Ministry recognized the fact that refugee claimants from Azerbaijan satisfied all the criteria for claiming the refugee status and that the denial of such a status would endanger them upon their return to Azerbaijan, but nevertheless, the Ministry refused to grant the refugee status. Namely, the Decision of the Ministry states that there was sufficient grounds to believe that their residence in Georgia was against the national interests of the country. [122] The Decision of the Ministry does not contain any substantiated argumentation on their decision, which partly rests on the determination (which is classified and not accessible to the parties) made by the State Security Service.

THE STATE SECURITY SERVICE WAS HANDED 2078 CASES ON THE GRANTING OF REFUGEE STATUS (AUGUST 1, 2015 - DECEMBER 2017)



2078 Number of IDPs from Georgia's occupied regions, cases of the The Ministry of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees of Georgia

993 Negative recommendations issued by the State Security Service

117 Law of Georgia on International Protection, Article 15(1)

118 *Ibid,* Article 17(1)

119 Internally displaced persons from Georgia's occupied territories, the Ministry of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees of Georgia, Letter N°04/07/10268.

120 *Ibid.*

121 see: *IPHR, Freedom now, EMC,* Repression Beyond Borders: exiled Azerbaijanis in Georgia https://emc.org.ge/2017/11/21/emcraport

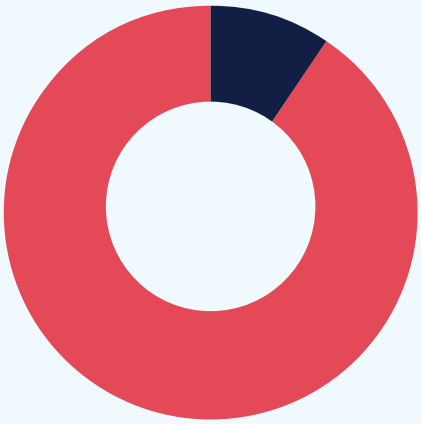
122 October 30, 2015 Decisino of the Ministry of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees of Georgia on the IDPs from Georgia's occupied territories.

One of the legal forms of residence on Georgian territory for a foreigner is a residence permit. There are various types of residence permits in Georgia, which vary depending on the criteria the claimant must meet. The issuing/renewal of residence permits is made LEPL Public Service Development Agency.

The Georgian government often rejects residence permits and extensions to Azerbaijani activists, journalists and politicians, based on subparagraphs (a) and (c) of Article 18 of the Law on Residence Permits, which is to say the applicant is believed to carry out activities that endanger state security and/or public order.[123]

The determination made by the Public Service Development Agency is generally based on largely classified information provided to it by the State Security Service or in the case of assessing public order, the Ministry of Internal Affairs. Accordingly, an interested party does not have access to the reasoning behind such determination.

THE STATE SECURITY SERVICE RECEIVED 72461 CASES ON DIFFERENT TYPES OF RESIDENCE PERMITS FROM THE PUBLIC SERVICE DEVELOPMENT AGENCY (AUGUST 1, 2015 - JANUARY 19, 2018)



72461	Number of cases handed to the State Security Service
7570	Negative recommendations issued by the State Security Service

The issuing of residence permits to foreigners who are critical or in opposition to other states can always potentially be viewed as coming as a hedge between the relationship of Georgia and another state. Therefore, this reasoning alone cannot be sufficient grounds for denying residence permits. Moreover, denying residence permits solely on this ground poses high risks of disproportionate interference in human rights.

In a setting when the parties are unable to offer substantiated argumentation for their decisions, the only mechanism for controlling the arbitrariness of the Government is the judiciary, which has access to the respective findings of the State Security Service and is therefore able to effectively monitor whether or not the decisions are substantiated and if they exclude any arbitrariness on behalf of the government.

Therefore, the control over the arbitrariness of the government depends on the good will of the judges and on how they will be able to use their inquisitive functions. It is also noteworthy that the practice of the general courts is not uniform. In one of the cases, the first instance of the court satisfied the lawsuit by the refugee claimant, but the appeal's court turned this decision over on March 21, 2017 based on new evidence (which was classified).[124]

123 See: IPHR, Freedom now, EMC, Repression Beyond Borders: exiled Azerbaijanis in Georgia, https://emc.org.ge/2017/11/21/emcraport

124 See: The sub-chapter of this report: The role of the public defender in the oversight over the State Security Service

3.7 BEST PRACTICE OF SELECTED COUNTRIES

Country	Structure	Mandate	Law enforcement powers
Germany	Each of its 16 states (Länder) has its own domestic security service. At the federal level there are three services: the Military Counter-Intelligence Service, the Federal Office for the Protection of Constitution and the Federal Intelligence Service.	The threats under the BfVs mandate do not include corruption or organized crime. The BfV is mandated to collect and analyse information on efforts: • directed against the free democratic basic order; • against the existence and the security of the Federation or one of its States; • aimed at unlawfully hampering constitutional bodies of the Federation or one of its States or their members in the performance of their duties; • jeopardizing foreign interests of the Federal Republic of Germany by the use of violence or the preparation thereof ; • directed against the idea of international understanding • The BND is mandated to collect and analyze information relating to important political, economic, and technical developments abroad, as well as abstract or concrete security of the Federal Republic of Germany and its citizens.	• The BfV is not given the powers to conduct criminal investigations and exercising law enforcement powers • The BfV is not given the powers to conduct criminal investigation BfV law outlines in detail the specific and circumstances under which the BfV is allowed to share information with the law enforcement agencies and exercising law enforcement powers • The BND Law explicitly bans the service from exercising police powers.

Canada	Civilian security/ intelligence agency (Canadian Security Intelligence Service-CSIS) Military intelligence service (Canadian Forces Intelligence Command) In addition, as part of its defense portfolio, Canada has set-up the Communications Security Establishment, mandated to collect foreign intelligence	The CSIS is mandated to 'collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada Neither organized /economic crime, nor corruption is included in the list of threats and thereby excluded from the mandate of the CSIS	The law represents best practice concerning the clear prohibition of law enforcement powers. Moreover, the Service cannot: (a) cause, intentionally or by criminal negligence, death or bodily harm to an individual; (b) willfully attempt in any manner to obstruct, pervert or defeat the course of justice; or (c) violate the sexual integrity of an individual.'
Croatia	Croatia has two security/intelligence services, one military (Military Security Intelligence Agency/ Vojna sigurnosno-obavještajna agencija -VSOA) and one civilian (Security Intelligence Agency (Sigurnosno-obavještajna agencija -SOA)	SOA collects, analyzes, processes and assesses the political, economic, scientific/ technological and security-related information concerning the foreign countries, organizations, political and economic alliances, groups and persons, especially those showing intentions, potential, concealed plans and clandestine activity directed against the national security, or other information relevant for the national security of the Republic of Croatia' The SOA's mandate is restricted to collection, analyzing and processing of data, thus it does not have investigatory functions. The SOA is obliged to share organized crime related data with police and prosecutorial authorities who are in charge of investigating those acts.	The SOA does not have law enforcement functions, it is not granted investigation, arrest and detention powers SOA officers can only interview persons, with expressly stated consent of the person, at the official premises of the SOA, by keeping interview records and making it available to judiciary and oversight bodies. SOA officials who obtain the necessary certifications to bear firearms, are permitted to use a firearm, only in exceptional circumstances to protect their own or another person's life, as well as in their capacity to protect state authorities, (including SOA itself), protected individuals, or critical infrastructure in the frame of their counterintelligence mandate.

Belgium	Belgium has two security/intelligence services: The General Intelligence and Security Service of the Armed Forces (GISS) which is the military intelligence agency; and the 'State Security' (Sûreté de l'État), which is the civilian security / intelligence service (hereinafter the Service) with both a domestic and foreign mandate	Mandate of the Service is as follows: • Research, analyze and process information related to all activities which threaten or may threaten internal security of the State and the continued existence of the democratic and constitutional order, the external security of the State, and international relations, the scientific or economic potential as defined by the National Security Council, or all other fundamental interests of the country defined by the King, on the proposal of the National Security Council; • Perform security vetting as entrusted to it upon directives of the National Security Council; • Research, analyze and process intelligence related to activities of foreign intelligence services on Belgian territory; • Perform any other duties entrusted to it by virtue of the Law.	• The Service is not allowed to investigate on its own the crimes falling under its mandate. However, if requested, the Service can provide technical support to criminal justice institutions in the framework of judicial investigations (e.g. terrorist cases) as long as it is carried out within the boundaries of protocols approved by the concerned Ministers • The Service does not have law enforcement powers, such as stop and search, arrest and detention, which is in line with international standards. • The Service has an 'intervention team', designated by the Ministry of Justice, for the sole purpose of protecting certain personnel and infrastructure of the Service. Members of this intervention team are given certain police powers, however the cases which they can apply those powers are very precisely defined in the law

3.8 SUMMARY AND RECOMMENDATIONS

The competencies of the State Security Service today are broad and vague and are not in line with international best practice. Therefore, the scope of authority of the Service should be decreased to an extent that is in line with its nature.

- The national security risks should be defined as per international standards, and it shouldn't include corruption-related and minor economic crimes. The competence of the Service should include the receival, processing and dissemination of information that supports respective persons in exercising operations related to protection of national security.[125]
- As per international standards and practice, the State Security Service should not have an investigative function and its purpose should not be the investigation of criminal cases, or the carrying out of specific investigative operations. The State Security Service should not have the mandate to issue an order to law enforcement agencies for an arrest to be made on their behalf.[126]
- The procedures for cooperation between the State Security Service and other respective investigative bodies should be defined by law. Namely, the law should specify the procedures through which the Service provides information on criminal cases to specific investigative bodies. The law should also define the guarantees of protection of the exchange of information.
- The State Security Service should not have law enforcement functions, which include a contact with citizens and the restriction of their rights in public space (for example: identification, questioning, etc.);
- The State Security Service should not have the power to have a temporary detention isolator;[127]
- The respective parliamentary committee should analyze the practice of the use of "ODR" institute'
- The grounds for denying residence permits and granting refugee status should be clearly defined by law. The conclusions of the State Security Service should be substantiated. The effective control mechanisms of the judiciary and the rights of the claimant should be strengthened.
- The special operative department should be stripped off its right to conduct secret surveillance and this right should be transferred to an institutionally-independent body, which will not have a professional interest in this regard;
- The legislation should specify the restriction of conducting secret surveillance towards a specific group of professionals, such as lawyers and journalists.[128]

125 UN Compilation of Good Practices, N°1

126 Germany has the best practice in this regard: See: German BfV law (Internal security services law), Article. 20-23 http://www.gesetze-im-internet.de/bverfschg/index.html

127 UN Compilation of Good Practices, N°30

128 See: Example of Belgium, The Organic Law on Intelligence and Security Services Article 2, As well as Germany, G-10 Law (Article 3.b)

CHAPTER 4. OVERSIGHT AND ACCOUNTABILITY OF THE STATE SECURITY SERVICE

The broad and unrestricted concentrated powers within the State Security Service require an existence of an effective mechanism for the balance and monitoring of these powers. The following specific factors define the necessity for exercising oversight over the Security Service:

- Security Services have the capacity to collect a huge amount of information through secret surveillance. This opens the door towards risks of abuse of power. The Venice Commission notes that Security Services "need to be adequately controlled by the executive in order to avoid that they develop a State within the State mentality"[129].
    - Security services have inbred in them a potential of abuse of State power. The subjectivity and flexibility of the notion of "national security", combined with its vital importance to the State, mean that governments have a wide margin of maneuver in this area [130]
- Security Services are financed from the state budget. They also frequently carry out classified procurements and therefore their spending are not transparent.

There is no single 'correct' model for the oversight of security services, however as per international standards, oversight should be comprehensive, and conducted by a number of actors including, the parliament, specialized bodies, the executive, judiciary, as well as civil society organizations[131]. The mandate and powers of such oversight actors should be carefully elaborated to ensure that there is no overlap and duplication among each other, while no aspect of the work of security services shall be left outside of the oversight system.

The involvement of various government bodies in the oversight process over the State Security Service is defined by the legislation. The Parliament, Government, General Courts, Prime-Minister, State Audit Office and Personal Data Protection Inspector are involved through various mandates in the process of oversight. However, multitude of actors in the oversight process doesn't necessarily equal to effective oversight. A clear example of this the rules for the appointment of the Head of the Service, where the risks of politically motivated appointment are high in spite of the involvement of various government branches in the process[132].

The forthcoming sub-chapters provide an overview of the powers and oversight practice of state bodies that exercise oversight over the State Security Service. Moreover, the sub-chapters present an international practice on the oversight of the security sector.

It should be noted that in addition to taking into account international practice on the formation of oversight over the Service, it is equally important to assess and analyze the threats and internal and external challenges of the country. Therefore, all decisions on the formation and mandate of the oversight body should be made with those threats taken into account.

4.1 PARLIAMENTARY CONTROL OF THE STATE SECURITY SERVICE

The Parliament is an essential component of an accountability system.

The main instrument of parliamentary control over the State Security System is the Defense and Security Committee and the activities of the Group of Trust. There are a number of Parliamentary oversight mechanisms over the State Security Service: Deputy inquiry/question; Appointment and dismissal of the Head of the Service; Summoning of the Head to the Faction, Committee or Plenary session; Hearing of the

129 European Commission For Democracy Through Law(Venice Commission)Report On The Democratic Oversight Of The Security Services, 2007, Paragraph 4 http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)016-e

130 Ibid, 5.

131 UN Compilation of Good Practices, para 13.

132 See: Second Chapter "Appointment of the Head of the Service", as well as Menabde.V, Papashvili.T, Kashakashvili.N, Kekenadze.G, Beridze.A, "Twenty Years Without Parliamentary Control", 2017 (Menabde et al. 2017), p. 126.

Report of the Service; Control of the Public Finances, etc.

As per international practice, the established mechanisms of parliamentary oversight are: Hearing of the annual report of the Security Service; Periodic meetings with management of agencies; Inviting management to give testimony; Inspecting premises of intelligence agencies.[133]

The majority of EU countries use expert bodies that are accountable to the Parliament to strengthen oversight over the security sector. At this time, 16 EU countries have expert bodies created for this purpose.[134]

Experts are not involved in the process of parliamentary oversight over the State Security Service. Moreover, the existing mechanisms of parliamentary control are in most cases formal and less effective.

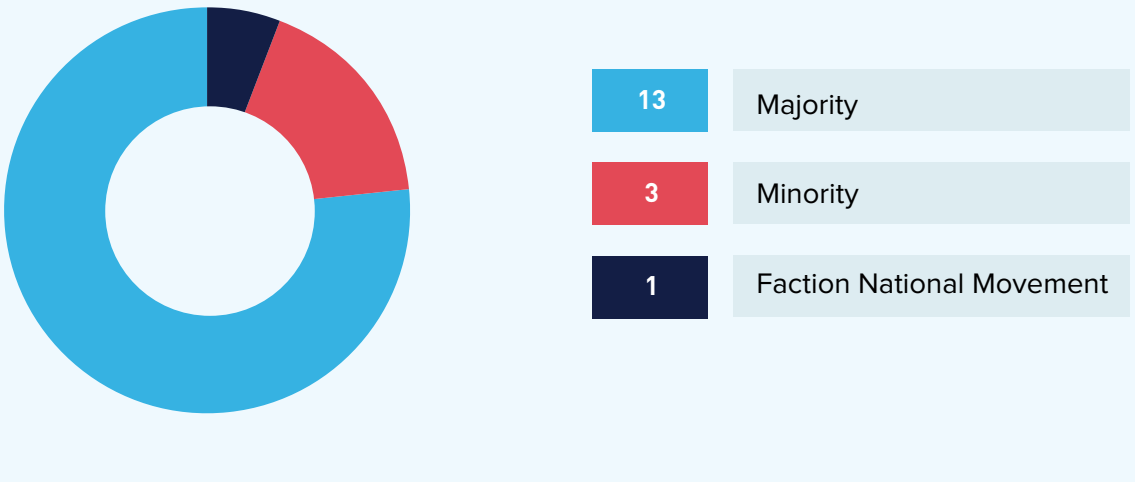
4.1.1 CONTROL OF THE STATE SECURITY SERVICE BY THE DEFENSE AND SECURITY COMMITTEE

The Defense and Security Committee works on issues related to defense and security in the Parliament. The limited mandate of the Defense and Security Committee and the Group of Trust do not provide a legislative basis for exercising effective oversight.

The composition of the committee is defined proportionally by the representatives of the factions and MPS that are not part of any faction.

During the 9th convocation, 17 MPs are members of the Defense and Security Committee, 13 out which belong to the parliamentary majority, 3 to the parliamentary minority, and one from the faction "National Movement".

COMPOSITION OF THE DEFENSE AND SECURITY COMMITTEE



In order to ensure cross-party membership in parliamentary committees, a great majority of European parliaments adopted the approach of proportional representation, while some countries provided additional guarantees for opposition and minority parties in such parliamentary oversight committees.[135]

133 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.135

134 See: EU FRA, *Surveillance by Intelligence Services Vol 2* (2017)p.68.

135 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), pp 92-95

For example, in Germany the Parliamentary Control Group, which conducts oversight over the security system, is comprised of 9 members, representing all parliamentary groups in the Parliament. Embodying best practice, the members are elected by a majority of the votes in the parliament.[136]

It is generally considered a good practice to grant chairpersonship of the Committee to the opposition.[137] In Croatia, for example, the internal policy and state security parliamentary committee, which exercises oversight over the security services and law enforcement, is composed of 13 members, which are chosen according to the general rules for the selection of members of parliamentary committees from members of parliament with an interest in national security matters. By law, the Committee is always chaired by a member of the largest opposition party.[138]

As per international standards, former employees of security services as members of such parliamentary committees are not recommended, especially in countries with a history of repressive security services.[139] According to Georgian legislation, the Defense and Security committee is formed as per the general rules of formation of committees. Therefore, there are no additional guarantees for the opposition nor are there any restrictions for MPs who are former employees of security services. Instead, the practice shows that the members of the committee are largely MPs with work experience in the security services.

According to Georgian legislation, the members of the Defense and Security Committee have the same access (except for members of the Group of Trust) to classified information as the members of other parliamentary committees. Only the members of the Group of Trust have access to classified information. The members of Group of Trust have to go through security clearance procedures to gain access to the classified information. The Council of Europe Commissioner for Human Rights has highlighted the crucial importance of access to information:

"[A]ll bodies responsible for overseeing security services [should] have access to all information, regardless of its level of classification, which they deem to be relevant to the fulfilment of their mandates. Access to information by oversight bodies should be enshrined in law and supported by recourse to investigative powers and tools, which ensure such access. Any attempts to restrict oversight bodies' access to classified information should be prohibited and subject to sanction where appropriate."[140]

There is no single approach in European countries towards this issue. In a great majority of European parliaments, MPs, especially members of parliamentary oversight committees are granted access to classified information. However, in most of those parliaments certain types of restriction are applied:

- "Need–to-know' principle" - According to this principle, persons can only access information if their official functions necessitate access to particular information, which applies in most parliaments
- Signing of a non-disclosure agreement
- Vetting of MPs before they are appointed to a parliamentary committee.141

It should be noted that vetting of MPs is not a recommended practice, since in most cases vetting of MPs is carried out by security services, which is supposed to be overseen by those MPs themselves. In cases where vetting is required by law, it is recommended to make the report of security services of advisory nature, and rest the final decision of appointment with the parliament.[142]

The MPs of the committees and its staff that exercises oversight over the state security services have access

136 See: https://www.bundestag.de/ausschuesse/ausschuesse18/gremien18/pkgr/einfuehrung/248044

137 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), para 176

138 Act On The Security Intelligence System Of The Republic Of Croatia, Article 205(4), See: https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

139 Venice Commission, *Democratic Oversight of the Security Services,* (2007), para 173

140 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.13

141 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.117

142 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015) p.44

to classified information in the following countries: Belgium, Estonia, Hungary, Czech Republic, Denmark, Germany, Latvia, Poland, Romania, Sweden, Lithuania, etc.[143]

In the following EU countries, there is unrestricted access to all types of classified information: Netherlands, Portugal, Norway and Slovenia. There is restricted access in the United Kingdom. In Romania, for example, the committee exercising parliamentary control has restricted access to information on ongoing operations, but has unrestricted access to information about finished operations.[144]

In Norway, all members of the committee have access to high-level classified information, as per national and NATO regulations. The committee members are bound by a duty of secrecy.[145]

It is important for the MPs of parliamentary committees (or other parliamentary oversight structural units) that exercises control to have full access to classified information. The oversight of a body, which has most of its information classified, is impossible without the existence of access to classified information.

The mandate of the Defense and Security Committee of Georgia is very broad and it addition to security, it also covers national defense and intelligence.

In 26 out of 28 EU member states, there is at least one parliamentary control responsible for oversight over the security sector. In certain countries, the specialized committee has an exclusive mandate for oversight over the security service. In some countries, the oversight function is exercised by a committee with a broad mandate that also covers law enforcement agencies.[146]

Throughout the Council of Europe area there is a trend towards vesting parliamentary oversight of security services in a single committee that exists exclusively for the oversight of security services.[147]

In spite of a broad mandate, the Defense and Security Committee of Georgia has very general powers over the State Security Service. The law doesn't allow the Defense and Security committee to use special mechanisms of control over the State Security Service (such as oversight over the collection of information, secret surveillance, protection of personal data within the security service, etc.). The Defense and Security Committee may use only the same mechanisms as other parliamentary committees (Summoning the Head of the Service to a session, hearing of a report).

According to the Rules of Procedure of the Parliament and the Statute of the Committee, the Defense and Security Committee has the following aims:[148]

- Exercises oversight over the regulation of the legislative base and adopted laws related to the government policy on state security;
- Drafts legislative initiatives, recommendations and proposals related to institutional reforms related to the security sector;
- Considers the ratification, ascension, denunciation and abolishment from international treaties related to the security sector;
- Hears the report by the Head of the State Security Service on the activities of the Service, drafts findings related to the activities to the Service and also prepares a draft resolution, which may include recommendations and proposals for solving/improving issues within the Service;
- Prepares findings related to the early termination of term of office of the Head of State Security Service.

143 See: Parliamentary oversight of Security and Intelligence Agencies in European Union http://www.europarl.europa.eu/ pg. 140

144 See: Parliamentary oversight of Security and Intelligence Agencies in European Union http://www.europarl.europa.eu

145 See: https://eos-utvalget.no/english_1/services/about_the_eos_committee_1/members/

146 EU FRA, *Surveillance by Intelligence Services Vol 2* (2017), p.66

147 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.42

148 See: Statute of the Defense and Security Commiteee http://parliament.ge/ge/ajax/downloadFile/50984/8.

- Signs memorandums of understanding with non-governmental organizations working on the security sector, to ensure civil participation in its activities

It is noteworthy that the Defense and Security committee does not effectively use the powers granted to it by the law. For example, during the reporting period, the Defense and Security Committee hasn't summoned the Head of the State Security Service.[149]

As per international best practice, committees, which exercise control over the security sector, are equipped with special oversight mechanisms. In some EU member states, in addition to the general mandate of oversight over the policy, administration and finances of the security service, the committees have the power to exercise oversight over finished special operations, and in certain cases – to exercise oversight over ongoing special operations.

Moreover, certain parliamentary committees in Europe have the mandate to exercise oversight over the specific aspects of the security service, such as oversight over operations related to information retrieval, use of personal information, as well as hearings of individual complaints against the service. In Germany, for example, there is a specialized security oversight committee that works on enforcing the legislation on secret surveillance. [150] In the period of two years, the committee received 65 petitions, 40 of which were about secret surveillance.[151] In Croatia, the mandate of the parliamentary committee includes the inspection of the legality of the activities of the service (including special operations on the retrieval of information through secret surveillance). Moreover, the committee holds a hearing of the individual complaints lodged against the security service.[152]

In 16 EU member states, in spite of the broad mandate of the parliamentary committees, specialized expert oversight councils are created, for the purposes of strengthening control over the security services. This is discussed in chapter 3.1.1.3.

4.1.2 GROUP OF TRUST

Forms of Parliamentary oversight over the State Security Service, in addition to main laws, are defined by the Law of Georgia on the Group of Trust. According to existing regulations, the Parliament establishes the Group of Trust within the Defense and Security Committee. The function of the Group is to exercise control over the secret activities and expenses of the special programs of the executive government.[153]

According to the Law on the Group of Trust, the Group is composed of 5 members:

- Chair of the Parliamentary Defense and Security Committee
- Member of the Parliamentary majority
- Majoritarian MP with most votes from the elections
- Member of the Parliamentary minority
- MP with most votes, who is not a member of neither majority nor minority

According to the law adopted on February 6, 2014[154], the Rules of Formation of the Group of Confidence were changed, namely, the provision of the composition of the Group being approved by a Resolution and the voting being public. Due to this rules of appointment, the previous convocation of the Parliament was unable to establish the Group of Trust for 2 years, due to the parliamentary majority refusing to support

149 January 5, 2018 N41/4-8 and July 19, 2017 N12109 Letters of the Defense and Security Committee, Also see: protocols of the committee sessions: http://parliament.ge/ge/saparlamento-saqmianoba/komitetebi/tavdacvisa-da-ushishroebis-komiteti-144/sxdomis-oqmebi1105/0/40;

150 *EU FRA, Surveillance by Intelligence Services (2015), p.37*

151 *EU FRA, Surveillance by Intelligence Services Vol 2. (2017), p.117*

152 *EU FRA, Surveillance by Intelligence Services (2015), p.70*

153 Also, exercise of other special powers, Law on Group of Trust, Article 1.

154 Amendments to the Law on Group of Trust, 19.02.2014, https://www.matsne.gov.ge/ka/document/view/2242496

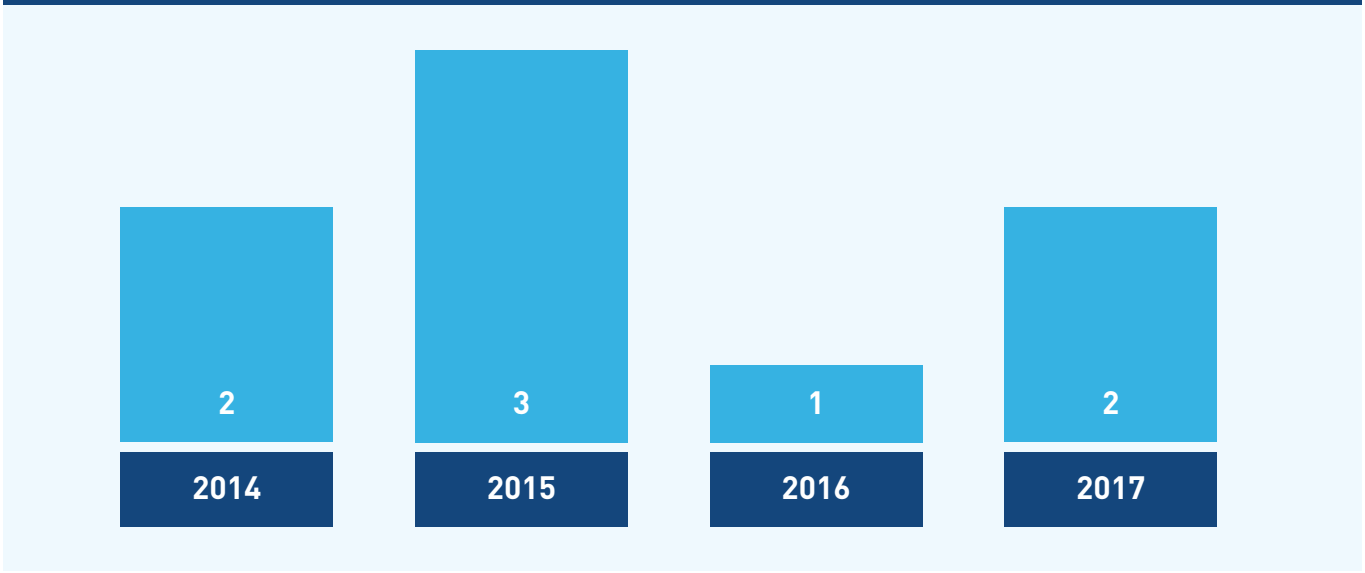
the candidate presented by the minority.[155] As a result, a political decision was made for amendments, according to which the Parliament takes note of the members of the Group of Trust and no hearing and vote is held.[156]

Nevertheless, the current rules of formation of the Group of Trust still doesn't guarantee the full formation of the Group. In the current convocation, the Group was formed on November 1, 2017 and it had 4 members[157], while the fifth member was to be an MP who is neither from the majority nor from the minority. Irma Inashvili from the Georgian Patriots and Salome Samadashvili from the National Movement were nominated for this position. Both candidates received the same amount of votes. The law does not envisage any exceptions for this case.

The sessions of the Group of Trust are held no less than twice every year. If required, additional sessions may be held by the initiative of its members, if the request is supported by a majority of the Group[158]. The requirement for a majority support may make it impossible for such a request for additional sessions to be granted to the minority representatives.

During the 8th convocation of the Parliament, the Group of Trust held six sessions. During the 9th convocation, the Group of Trust was formed on November 1, 2017, but held only two sessions[159]. On the second session, which was held on December 1, the Group invited the Head of the State Security Service, Vakhtang Gomelauri, who presented information on the large-scale anti-terrorist operations held in Tbilisi[160]. Notably, the mandate of the Group of Trust extends only to the budgetary control of the Service and it's not within the Group's competence to receive information on anti-terrorist operations.

NUMBER OF MEETONGS OF THE GROUP OF TRUST SINCE 2014



155 Candidate was Giorgi Targamadze from the United National Movement

156 The aforementioned subjects present the nominated candidates for the Group of Trust to the Parliament. The candidates from the Majority and Minority are presented by the leaders of the Majority and Minority, the deputies elected through the majoritarian system are presented based on agreement, while deputies beyond the majority and minority are presented through the agreement made by those who had given consent to presenting them. Deputies elected through the Majoritarian system and the deputies who are neither majority nor minority members, through their respective quotas, can sign a support letter only for one candidate.

157 Irakli Sesiashvili – Chairperson of the Committee, Eka Beselia – Majority, Archil Talakvadze – Majoritarian MP, Irakli Abesadze – Minority: http://www.parliament.ge/ge/saparlamento-saqmianoba/komitetebi/tavdacvisa-da-ushishroebis-komiteti-144/ndobis-djgufi/djgufis-wevrebi

158 Law on Group of Trust, Article 10

159 https://goo.gl/M5dKQB

160 Meeting of the Group of Trust, 1.10.2017, https://goo.gl/8MtfiD.

The extension of the scope of authority in 2015 of the Group of Trust to the control over the state procurements was a positive step forward. A similar obligation was envisaged for the MIA in reporting to the Group of Trust on any procurement or services that exceed 2 million GEL[161]. The State Security Service does not a have a similar obligation.

As a result of the amendment carried out in March 2017, the LEPL Operative-Technical Agency has to present an annual statistical and general report to the Group of Trust[162].

The Group of Trust has the right to inspect the activities of the Operative-Technical Agency, **no more than twice per year**[163]. For the purposes of the inspection, the Group of Confidence picks one member from its composition, by the rules defined in the Law of Georgia on the Group of Trust. The Group of Trust has the right to present recommendations to the Operative-Technical Agency on how it may improve its performance. The Group of Trust is obliged to address the respective law enforcement body and provide them with any supporting documents, should any violation be found during the inspection of the Operative-Technical Agency.

Notably, the law defines the right of the Group of Trust to hold an inspection, rather than an obligation. The Group of Trust takes its decisions based on majority vote, therefore the ruling political power always represents the majority within the Group. Due to this, the provision stipulating the right to hold an inspection can be seen as an ineffective mechanism. It is also unclear why there is a maximum threshold for the number of times the Service can be inspected, especially when there may be situations when more inspections are required.

The Group of Trust is the only parliamentary structure that has clearance to classified information, which is an important factor for oversight over the security service. However, the mandate of the Group of Trust doesn't guarantee for a complete oversight over the State Security Service, since the clearance to classified information is limited to budgetary control.

Lack of sufficient human resources are another problem for the activities of the Group of Trust. The control over the classified procurement implies access to multi-million worth of contracts and procurement documentation. For example, during 2010-2015, the total amount of classified procurement exceeded 700 million GEL[164]. Naturally, the analysis of this volume of information is a demanding task. As noted above, the scope of the Group of Trust was expended in March, 2017 and it now also includes inspection of the activities of the LEPL-Operative-Technical Agency. In spite of this, only one person is employed in the parliamentary cabinet of the Group of Trust. Due to this, there is grounds to suspect that the Group of Trust doesn't have the sufficient human resources to effectively exercise its functions.

4.1.3 INDEPENDENT OVERSIGHT OF SECURITY SERVICES – THE ROLE OF EXPERT OVERSIGHT BODIES

Over the past decade, there has been a growing tendency among democratic countries for establishing expert oversight bodies to enhance security sector accountability. Expert oversight bodies are independent institutions set-up exclusively for the purpose of overseeing security services, operating with full-time staff who are entrusted with necessary powers and resources. In this regard, the Human Rights Commissioner of the Council of Europe stated that expert oversight bodies 'are often best placed to conduct detailed day-to-day oversight of the legality of security service activity'. As of December 2017, 16 out of 28 EU member states have established such bodies[165]. Below is a brief overview of international standards on the key features of expert oversight bodies.

Institutional set up: Although the way expert oversight bodies are set-up varies, in most countries such a body is established by the Parliament and it is accountable to the respective parliamentary oversight committee.

161 Article 6(4) of the Law on Group of Trust

162 Ibid, Article 6[1].

163 Refer to Chapter 3.4 for the inspection of the activities of the LEPL – Operative-Technical Agency of Georgia

164 Classified Procurement Rules, Georgian Young Lawyers Association, 2017, p. 3.

165 *EU FRA, Surveillance by Intelligence Services Vol 2, (2017)* p.68

Composition: Expert oversight bodies are composed of specialists, often non-political and highly respected senior figures who are selected based on their expertise and qualifications. They are usually given fixed term tenures, which is an important safeguard for their independence. Since such bodies are often mandated to oversee the legality of services' activities, a common international standard is that at least one member of the body should have a legal background (senior lawyer or a former judge/prosecutor).[166] However, it is also recommended that expert oversight bodies should, to the extent possible, be composed of members with diverse backgrounds in order to effectively oversee increasingly technical and complex work of security services.[167]

Mandate: As per a common standard, expert oversight bodies are mandated to oversee the legality of the activities and policies of security services, including their compliance with human rights.[168]

As per the practice in European countries, oversight councils are accountable towards specialized parliamentary committees, however they still have strong guarantees of independence in fulfilling their activities. For example: to invite Heads of the Security Service; to independently study an issue; to request information for the purposes of fulfilling specific oversight functions; to summon officials; to inspect the premises of the security service, without the consent of the committee (for example: in Germany and Belgium), as well as making its investigation reports public.[169]

One of the main functions of the expert oversight bodies is the exercise of oversight over the secret surveillance, which can be exercised prior to the surveillance taking place or in the aftermath. The councils have the following powers to exercise oversight over secret surveillance operations:

- Ex-ante authorization/approval: Ex-ante oversight may either take the form of expert body actually authorizing the warrant or the body approving a signed warrant before it enters into force[170], thereby substituting or complementing judicial oversight
- On-going oversight: scrutinizing the information collection process, and checking compliance with the warrant,
- Ex-post oversight: reviewing the retention, use, and sharing of personal data by security services[171]

It should be noted that ex-ante authorization/approval of surveillance measures by expert oversight bodies is not yet common in EU member states. Only Germany, Belgium and Austria adopted this approach so far, while in other countries, ex-ante authorization of targeted surveillance lies with the judiciary.[172] Most expert bodies in Europe focus on ongoing and ex-post oversight of targeted surveillance measures.

In most of the countries, the mandate of the expert oversight bodies also includes the hearing of complaints lodged against the security services. As per UN Compilation of Good Practices, the hearing of the complaints represent a best practice and is an important function for the oversight body.[173]

The UN Compilation of Good Practices has set clear standards for powers and methods of oversight institutions:

'Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law

166 Venice Commission, *Democratic Oversight of the Security Services,* (2007), para 228, Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p.97

167 Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015), p.50, Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p. 101

168 Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015) p.47

169 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.20

170 *EU FRA, Surveillance by Intelligence Services Vol 2. (2017)* p.94

171 Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015)p. 49,

172 *EU FRA, Surveillance by Intelligence Services (2015),*p.52

173 UN Compilation of Good Practices, Practice 9

enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.' [174]

This important UN standard has crucial aspects, which necessitates further analysis:

1. *Initiate own investigations:* The significance of this power is also recognized by the Venice Commission, which recommends that expert bodies should be able to decide on their agenda, determine priorities for oversight, and launch investigations on their own initiative.[175] This way they are not bound by overseeing only the aspects that the government or the parliament orders them. In line with this standard most expert bodies have the power to launch own-motion investigations.

2. *Access to information*: In order to carry out their mandates effectively, expert oversight bodies should be given extensive access to information. While it is typical that the law imposes certain l restrictions to their access (for instance overseers may not be allowed to access information on the sources of security services, or on ongoing investigations) such limitations should be defined in the law in the narrowest sense, otherwise it could lead to the executive imposing arbitrary restrictions to access information, which seriously obstructs the work of expert oversight bodies. [176] An important standard that enhances oversight bodies' access to information is to legally oblige security services and the executive to proactively disclose information to the overseers [177], especially on surveillance measures. However, it should be noted that access to information comes with certain responsibilities. As per UN Compilation of Good Practices, '[O]versight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions'. [178] Most commonly members and staff of such expert bodies go through security clearance procedures.

3. *Full cooperation of intelligence and law enforcement agencies:* In the framework of their mandates, most expert oversight bodies are tasked with conducting inspection to the facilities of security services, investigating complaints and scrutinizing the implementation of surveillance measures by security services. Accordingly, such expert bodies should either be given the power to compel intelligence and law enforcement cooperation in their investigations or the expert oversight body itself should be entrusted with certain investigatory powers. The absence of such powers would render the expert oversight body 'toothless', left at the willingness of intelligence services to cooperate.

International experience shows that parliamentary committees with broad mandates are unable to meet the challenges related to the oversight over the State Security Service. Globally, there seems to be a growing preference for expert oversight bodies[179]. Such bodies allows for greater expertise and time in the oversight of security and intelligence services. [180] Having fixed tenures, they are able to provide continuous oversight as opposed to parliamentary oversight bodies, which in most cases stops functioning when the parliament is in recess or dissolved for election.[181] However establishing expert oversight bodies with extensive mandate and powers requires significant human and financial resources. Moreover, the formation of these bodies is not dependent on a political cycle and therefore it has a higher quality of independence and integrity.

174 Ibid, Practice 7

175 Venice Commission, *Democratic Oversight of the Security Services* (2007), para 229

176 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p 123-124

177 Ibid, p.127

178 Ibid, p.127

179 See: Parliamentary oversight of Security and Intelligence Agencies in European Union http://www.europarl.europa.eu/

180 Venice Commission, *Democratic Oversight of the Security Services* (2007), para 219

181 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011)), p.90

4.1.4 PARLIAMENTARY HEARING OF THE STATE SECURITY SERVICE REPORT

The Head of the Service or the deputy head submits a report on the activities of the previous year by the Service to the Parliament of Georgia once a year, no later than April 15.[182]

In addition to the obligation to present the annual report, the Head of the Service is obliged to present a performance report within two weeks after the report was requested.[183]

After considering a report on implemented activities of the State Security Service, the Parliament shall evaluate the performance of the Service with its decree. This decree may include recommendations and proposals on addressing specific shortcomings and/or improving performance of the Service. After considering a report on implemented activities of the State Security Service, at least one-third of enlisted MPs may raise an issue on pre-term termination of powers of the Head of State Security Service. The final decision is made through ballot with support of majority of the full composition of the Parliament.

The presentation of the first report by the State Security Service's Deputy Head, Levan Izoria, took place on March 29, 2016 at a joint session of three committees[184]. Notably, according to the legislation of that time, only the Head of the Service could present the report, therefore the requirements of the Law on State Security Service were breached. [185]

The report focused on the situation in the occupied territories, counter-intelligence activities, fight against terrorism, cyber-security, analytical work and fight against corruption[186]. Notably, the report was not heard during a plenary session. [187] This indicates that the Parliament did not thoroughly use its oversight function and did not use all the mechanisms granted it to by the law. [188]

On April 13, 2017, the joint session of committees held a hearing of the 2016 report[189] of the State Security Service, which was presented by the Deputy Head Aleksandre Tabatadze. A few weeks prior to the presentation, on March 22, the Parliament adopted changes to the Law on State Security Service and granted the Deputy the right to present the report. Therefore, unlike from the previous year, no law was violated with the presentation of the report.

Notably, unlike from the previous years, the committee hearing of the report was held behind closed doors. The plenary session on the report was also not public. In spite of the fact that the Parliament formally carried out its oversight procedures, it's hard to tell how substantial their engagement in their process was. It is important for there to be a legal reason behind holding the hearings behind closed doors, especially when there could not have been any classified information in discussion since there were MPs present who don't have clearance to classified information.

Notably, upon the end of the session the Parliament assessed through a Decree the report of the Service. The Decree consisted of one sentence: "The 2016 report of the activities of the State Security Service are positively assessed".[190]

During the reporting period, the Parliament of Georgia did not request the Head of the Service to hold an extraordinary presentation of a report.

---

182 Article 8 of the State Security Service, Article 229[6] of the Rules of Procedure of the Parliament

183 Rules of Procedure of the Parliament of Georgia, Article 229[6]

184 The State Security Service reporting to the Committees on activity for 2015, March 29, 2016, https://goo.gl/Kqizyo.

185 See in detail: Menabde et al. 2017, p. 129.

186 http://www.parliament.ge/ge/ajax/downloadFile/44943/5635_SSSG_REPORT. The presented information was assessed as broad and less informative by then-Chairperson of the Legal Issues Affairs Committee Vakthan Khmaladze, however the reason according to him was the open hearing. Vakthang Khmaladze stated his opinion on the initiation of the legislative amendments, which would establish standards for presentation of specific reports by agencies.

187 The March 30, 2016 plenary session wasn't held due to lack of quorum (https://goo.gl/fi5izP), while the May 12 report was delayed (https://goo.gl/uqUnmD) and hasn't been held to date

188 Menabde et al. 2017, p. 130.

189 The Committees to hear the Report by the State Security Service, April 13, 2017 https://goo.gl/6ZYFQu.

190 April 19, 2017 Decree N635-II of the Parliament, https://info.parliament.ge/file/1/BillReviewContent/149429?

Hearing of reports by the State Security Service is one of the most important mechanisms of parliamentary control over the Service. In order to effectively carry out such oversight activities, parliamentary committees should be provided with sufficient powers, most notably the power to access information.[191]

The annual report presented by the State Security Service to the Parliament is so broad that it is impossible to have a clear picture about its activities and therefore it is not possible to exercise effective oversight. The formal nature of the presentation of the reports is due to the format of the hearing and the oversight body's low quality of clearance to classified information.

Although there is no internationally recognized standard for the content and the length of the annual reports of services, good practice suggest that it should include:[192]

- Key priorities of the service;
- Overview of major security threats;
- Substantial changes to security/intelligence related policies;
- Information and statistics on the accountability functions, including its response to requests for access to information.

The 2015 report included information on the following issues:

- Occupied territories
- Counterintelligence activities
- Fight against terrorism
- Cyber security
- Chemical, biological, radiological and atomic security, fight against dissemination of weapons and materials of mass destruction
- Fight against corruption
- Analytical activities
- Protection of personal data, accessibility of public information
- Human resources, material-technical database
- Interagency and international cooperation

The 2016 report is broken down into the same issues as the report of the previous year. Both reports are general and provide several types of information: prevention of incidents and the response mechanisms through the hot line; information on the denial/approval and checking of physical and legal persons on access to classified data; information on border control for the purposes of counter-terrorism; information on operations related to the protection of chemical, biological, radioactive and nuclear security; information on the disciplinary proceedings within the State Security Service; information on civil servant offenses.

Both reports contain statistics on the release of public information, which only includes information about the amount of information requested, amount of public information released, number of denials for the release of the public information and the number of requests transferred to other bodies. Notably, the service doesn't fulfill the obligation defined in the General Administrative Code, according to which a public

191 UN Compilation of Good Practices (2011), Practice 7

192 Laurie Nathan, 'Intelligence Transparency, Secrecy and Oversight in a Democracy', p.55 in Born and Wills (ed.) Overseeing Intelligence Services: A Toolkit (DCAF: 2012), p.57

institution is obliged, on December 10 each year, to publish a report on the release of public information, which should also include other associated information.[193]

The report doesn't provide detailed information on the grounds of which the requests were denied. Moreover, the report doesn't contain the obligatory statistics defined by the General Administrative Code, which would be useful for establishing a sustainable practice, especially in light of the fact that the Service systematically processes classified information and that an established practice would be critically important for the effective fulfillment of freedom of information.

4.1.5 THE USE OF MECHANISMS OF PARLIAMENTARY CONTROL OVER THE STATE SECURITY SERVICE (DEPUTY QUESTIONS/INQUIRY, SUMMONING TO SESSIONS, ETC.)

One of the important mechanisms for parliamentary oversight is the deputy/questions by an MP, faction or a group of ten MPs. During the 8th and 9th convocation of the Parliament (from August 1, 2015 to October 2017), three deputies, who all belong to the opposition parties, sent a total of five questions to the State Security Service.

The State Security Service responded to all five questions. In one instance, the question was redirected to the Ministry of Internal Affairs[194].

The deputy questions related to the request to receive information on the staff (names, surnames and positions) [195] of the bodies (full-time and part-time) subordinate to the State Security Service. Moreover, the questions requested information on the autobiographies and CVs[196] of the Head and Deputies of the State Security Service and Heads and Deputies of the Counter-Intelligence Departments. In both cases, the responses noted that the aforementioned information is personal data and that it wouldn't be provided. In another question, the MP requested information on a criminal case[197] and the extradition of a foreigner from the airport[198].

Only five deputy questions[199] during two years indicates that this mechanism of control is rarely used. The reason for this might be the low quality of the responses. For example, as noted above, the Service deemed CVs of the Heads of its departments as classified information and refused to release the information.

According to Article 59(2) of the Constitution of Georgia, a group of at least ten members of the Parliament or a Parliamentary Faction shall be entitled to apply with a question to any body accountable to the Parliament, the Government, a particular member of the Government the latter being obliged to answer the raised questions at a sitting of the Parliament. The answer may become a matter of discussion of the Parliament. The date of response for each question is the last Friday of every month – the Government Hour. [200]

It is interesting that the government hour was not held during the 8th and 9th convocations, because neither ten members of the Parliament nor a Parliamentary Faction have posed a question.

---

193 See Article 49 of the General Administrative Code of Georgia: The report should include the following information: a) the number of applications submitted to a public institution for issuing public information and making amendments to public information, as well as the number of decisions on rejecting such applications; b) the number of decisions on granting or rejecting applications, the name of the public servant making the decisions, as well as the decisions on closing its own session by a collegial public institution; c) the public databases, and collecting, processing, storing and transferring the personal data by public institutions to others; d) the number of violations of the requirements of this Code by public servants, and imposing disciplinary fines on the responsible persons; e) the legislative acts used by a public institution as a basis for refusing to issue public information, or when closing the session of a collegial public institution; f) appealing decisions to refuse issuing public information; g) the costs, including the amounts paid in favour of a party, related to processing and issuing information by a public institution, as well as to appealing decisions to refuse to issue public information or to close the session of a collegial public institution

194 State Security Service Letter to the MIA, 24/07/2017, https://info.parliament.ge/file/1/TrashContent/2333?token=

195 Deputy Question N07-4/598/8, https://info.parliament.ge/#mpqs/598.

196 Deputy Question N07-4/640/8, https://info.parliament.ge/#mpqs/640.

197 Deputy Question N07-4/90/9, https://info.parliament.ge/#mpqs/907.

198 Deputy Question N07-4/112/9, https://info.parliament.ge/#mpqs/929.

199 In this time period, up to 700 deputy questions were sent

200 Article 221 (2) of the Rules of Procedure of the Parliament

According to the Constitution of Georgia, a member of the Government, an official elected, appointed or approved by the Parliament, shall be entitled and in case of request shall be obliged to attend the sittings of the Parliament, its Committee or Commission, to answer the raised questions at a sitting and submit an account of an activity. [201] The aforementioned persons are also obliged attend the sitting of a faction, answer the questions asked during the sitting and report on the work done.[202] The obligation to attend committee and commission sessions is also defined in the Law on State Security Service.

During the reporting period, the Head of the State Security Service was not summoned to a plenary, committee or commission session.

During the 8th and 9th convocations of the Parliament, there were three attempts to exercise oversight over the State Security Service through summoning of the Head of the Service. Namely, the factions within the parliamentary minority summoned the Head of the Service, Vakthan Gomelauri, once in 2015, as well as twice in in February and July of 2017. Nevertheless, the Head of the Service did not show up for any of those summons[203].

4.1.6 BEST PRACTICE OF SELECTED COUNTRIES:

Parliamentary control:

Country	Who controls	Sphere of control	Composition/ rules of selection	Access to confidential information	Mandate, authority
Germany	Specialized parliamentary committee 'Parliamentary Control Panel'	Mandated to oversee the activities of all federal security services	9 members, representing all parliamentary groups in the Parliament. Elected by a majority of the votes in the parliament. Chairpersonship of the Panel rotates every year between a member from the governing party and an opposition party.	Empowered to require the Federal Government and security services to submit files and transmit electronic data.	• Oversee policies and finances of security services • Mandate to receive and handle individual complaints against security services • Tasked with regularly receive information on internal policies and the implementation of surveillance laws • Oversight over the implementation of legislation on secret surveillance

201 Article 60 of the Constitution of Georgia
202 Rules of Procedure of the Parliament of Georgia, Article 94
203 Information retrieved through FOI: N18403

Canada	National Security and Intelligence Committee of Parliamentarians	Security Service	The Committee is composed of 11 members (3 senators and 8 elected MPs). There is no proportional representation of parties, but the law guarantees 3 out of 8 seats for opposition party members	The Committee is entitled to 'have access to any information that is under the control of a government department and that is related to the fulfillment of the Committee's mandate..	The committee has a broad mandate, and tasked with overseeing 'the legislative, regulatory, policy, administrative and financial framework for national security and intelligence' as well as 'any activity carried out by a department that relates to national security or intelligence, unless the activity is an ongoing operation'
Croatia	Parliamentary Committee for Interior Policy and National Security ,	Security services and law enforcement bodies	The Committee is composed of 13 members, chosen according to the general rules for the selection of members of parliamentary committees from members of parliament with an interest in national security matters	The Committee members have the right to access classified information, however they must obtain clearance certificate	• reviewing the legality of activities of the services (including special measures for covert information collection) • overseeing financial management • reviewing Ombudsman's report • Mandated to receive and handle individual complaints against the SOA
Belgium	Special Committee	Security service	The Committee is composed of 14 members of the Chamber of representatives based on proportional representation.	Access to confidential information	The parliamentary committee drafts and reviews bills, examines the annual activity report of the Standing Committee I and scrutinizes its draft budget, and examines the bi-annual investigation reports of the Standing Committee I

Independent oversight councils:

Country	Name of the council	Composition/ appointment rules	Mandate, authority
Germany	G-10 Commission	The G-10 Commission is composed of four members, appointed by the Parliamentary control Panel upon consultation with the Federal Government. No restriction for membership on current MPs	• Ex-ante approval of surveillance measures • Oversee the entire processes of collection, handling and the use of personal data by security services; • Receive and investigate complaints against services with respect to surveillance practices and protection of personal data
Croatia	'Council for the Civilian Oversight of the Security Intelligence Agencies	The Council is composed of a chairperson and six members, all appointed by the Croatian Parliament, on the basis of a public call and selection based on qualifications.	• Mandated to oversee the legality of the work of the security services as well as to monitor and supervise the application of surveillance measures • Monitoring and oversight over secret surveillance use • Mandated to receive and handle complaints concerning unlawful procedures or misconduct of security and intelligence agencies • Power to launch investigation upon complaints and at the request of any state body

Belgium	Two separate bodies - the Administrative Commission and the Standing Intelligence Oversight Committee	The Administrative Commission is composed of a state prosecutor and two judges The Committee is composed of two members and a chairperson, all appointed by the Parliament	• Oversight over the State Security Service; • Upon complaints, requests by the Parliament or judicial authorities, carries out investigations, including investigations against members of the services who are suspected of having committed a felony or misdemeanor; • Serves as an appeal body for security clearances. • Entitled to launch investigations on its own initiative • Overrule a positive decision by the Administrative Commission on a surveillance request
Canada	**Security Intelligence Review Committee (SIRC)**	The SIRC is composed of five members headed by an executive director.	• Overseeing the service's compliance with the law, policies and internal regulations, • Scrutinizing the activities of the service and investigating complaints • In conducting investigations, the SIRC has judicial powers to the same extent as a superior court; such as summoning and enforcing appearance of persons, summoning written documents and evidence • The SIRC can 'direct' the security service to conduct a review of the service's activities

4.1.7 SUMMARY AND RECOMMENDATIONS

Parliamentary control over the State Security Service is one of the most important components of oversight. In Georgia, parliamentary oversight over the State Security Service is a formal procedure, which is conditioned due to lack of legislative guarantees and traditions of real oversight over the security services.

Over the past decade, there has been a growing tendency among democratic countries for establishing expert oversight bodies to enhance security sector accountability. Due to the increasing volume and complexity of activities of the security services, there is no doubt that it is impossible for parliamentary

committees to exercise effective oversight without the involvement of experts. There are a number of weak points in having only MPs exercise parliamentary oversight. First of all, parliamentary committee oversight carries risks of politicization of the security services. Moreover, as a rule, MPs don't have sufficient time, resources and knowledge to exercise effective oversight over the security services, especially in operations such as secret surveillance.[204] There seems to be a growing preference for expert oversight bodies that are accountable to the Parliament.

As per international best practice, the following points are crucial for strengthening parliamentary control over the security services:

- A specialized full-fledged parliamentary structure for oversight over the security system (standalone committee, sub-committee or Group of Trust with broadened mandate) carries out the control of the policy and all activities of the state security service (including giving consent to procurements exceeding a certain threshold). The members of the committee should be elected by the Parliament.
- The parliamentary committee exercising control over the state security service should establish a permanent expert oversight council, which will systematically control the security service and be accountable to the Parliament. The members of the oversight council should be elected by the Parliament.
- The members of the specialized parliamentary committee and oversight council should have full clearance to classified information. Exceptions can be made on information related to ongoing operations. The members of the committee and oversight council should undergo security clearance. The conclusions made to the Parliament by the Security Service should be recommendatory, while the conclusions from the experts should be obligatory.
- The oversight council should have the following powers:
    - To conduct planned and ad hoc visits to the premises of the State Security Service and its subordinate structural units;
    - To hold a hearing of the annual report of the State Security Service and request extraordinary presentations of the report, including on ongoing operations and secret surveillance;
    - To have access and analyze the classified documents and materials stored in the agencies
    - To conduct control over the public finance expenditures of the Service, including issuing consent to classified state procurement above a certain threshold
    - To conduct an audit of the technical equipment held by the Service and its subordinate structural units
    - To summon officials, experts and interested persons to the sessions
    - To receive and analyze statements, complaints, including on secret surveillance, related to its scope of activities
    - To control the protection of personal data within the State Security Service
    - To address the Parliament of Georgia with a recommendation/conclusions on the violations and problems within the State Security Service, including on the dismissal of the Head of the Service, as well as establishing a special parliamentary investigative commission
- While it's true that the oversight council is accountable to the Parliament, it should have guarantees of independence. For example, it should have the right (without the consent of the Group of Trust) to invite the Head of the Service, to independently begin the analysis of an issue, to request information, to summon officials, to conduct visits to the premises of the security service (without the consent of the Group of Trust), as well as have the right to make the report presented to the Parliament public.

204 Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, (DCAF: 2010), pp.42-43

4.2 JUDICIAL OVERSIGHT OF SECURITY SERVICES

Judicial oversight is an integral part of the accountability systems of security sector. The State Security Service employs covert methods of collection of information both for investigation and counterintelligence purposes, which methods are closely connected with the right of an individual to private life (right to privacy). Judicial oversight of State Security Service is of particular importance in the light of human rights.

The international actors, including the UN special Rapporteurs, Council of Europe's Venice Commission and Commissioner for Human Rights, as well as the EU strongly emphasize the importance and necessity of judicial oversight of security authorities. In its case law the ECHR stresses, that *"The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure."*[205]

Council of Europe's Venice Commission explains: *"The guarantees of prior judicial control subordinate security concerns to the law, and as such they serve to institutionalize respect for the law."*[206]

According to international practice judicial control of security services is undertaken in three main directions:

- Prior control of measures, restricting human rights (prior authorization);
- Review of claims filed against authorities and restitution of rights;
- Oversight of ongoing covert operations.

Pursuant to the law of Georgia, the State Security Service requires a judicial authorization for the conduct of following measures:

- Covert investigative activities[207] - electronic surveillance[208] - definition;[209]
- Request of electronic communication identification data from an authorized agency[210]
- Control of mail correspondence[211]

The State Security Service does not require judicial authorization for the conduct of the following covert measures:

- Covert audio and video recording for counterintelligence purposes;
- Covert filming and photography for counterintelligence purposes;
- Use of telecameras and other electronic devices;
- Strategic monitoring operation;
- Individual monitoring operation;
- Agreed electronic surveillance - electronic surveillance under written consent of one of the parties to a telephone or other electronic communication;
- Infiltration of an undercover agent into a criminal group.

---

205 Klass v. FRG http://hudoc.echr.coe.int/eng?i=001-57510 para 55.

206 Venice Commission, *Democratic Oversight of the Security Services* (2007) Para. 214

207 Wiretapping and recording telephone communication; interception and recording of information from a communications channel, computer system and installation of respective software in computer system to this end; determination of geolocation in real time; monitoring of mail and telegraphic communications; covert video and/or audio recording, filming and photography; electronic surveillance through technical means, which do not endanger human life, health and the environment. Code of Civil Procedure of Georgia. Article 143^1.

208 Wiretapping and recording telephone communication; interception and recording of information from a communications channel, computer system and installation of respective software in computer system to this end; determination of geolocation in real time for counterintelligence purposes. (Will come in force from 30 March, 2020. Law of Georgia on Counterintelligence Activities.

209 Will come in force from 30 March, 2020.

210 Law of Georgia on Counterintelligence Activities, Article 14^7.

211 Law of Georgia on Counterintelligence Activities, Article 16.

Below chapters will offer the detailed overview of the modes of judicial oversight of different covert measures.

4.2.1 JUDICIAL OVERSIGHT OF COVERT INVESTIGATIVE ACTIVITIES

The wide mandate of the State Security Service also delegated it with investigative powers. Respectively, acting within its terms of reference the Service may conduct any investigative action, including covert investigative actions, in accordance with the procedure, prescribed by the Code of Criminal Procedure of Georgia.[212]

A secret investigative action[213] is conducted on the basis of a ruling of a judge. In urgent cases, when a delay may result in the destruction of important for the case factual data or render it impossible to obtain these data, a covert investigative action may be launched without a ruling of a judge, but rather on the basis of prosecutor's reasoned decree. In this case the prosecutor is required to apply to the court of law within 24 hours, which should review the motion not later than within 24 hours following the submission thereof. A judge makes a decision on the recognition of conducted covert investigative action either legal or illegal, its termination, cancellation of the results or destruction of the materials/data obtained through it.

Amendments, made to the Code of Criminal Procedure on the first of August, 2014 considerably improves the standard of protection of human rights in the course of wiretapping:

- It was established that secret surveillance and wiretapping is allowed only after launching the investigation.[214]
- The group of persons was identified, against whom a covert investigative action can be undertaken - a person directly linked with a crime or a person who receives or communicates information intended for or stemming from a person directly linked with a crime, or a person directly linked with a crime, who uses communication means of the person concerned;
- Maximum length of a covert investigative action was defined - one month, which can be extended under a ruling of s judge, but not more than up to 6 months.
- The mode of destruction of obtained data and the obligation of notification of the person, against whom the covert investigative action was conducted, was established.

Amongst these amendments was the obligation of the Supreme Court of Georgia to maintain the register of secret investigative measures and publish relevant information by the end of each year.

Statistics

Statistics of secret surveillance and wiretapping[215]

Year	Reviewed motions	Fully upheld motions	Motions upheld in part	Denied motions	A motion for the extension of the period of wiretapping and recording a telephone conversation
In 9 months of 2017	404	366	20	18	Reviewed - 138 Upheld - 124 Upheld in part - 11 Denied - 3

212 Code of Criminal Procedure of Georgia, Chapter XVI[1].

213 See footnote 112.

214 Until the first of August, 2014 secret surveillance and wiretapping was regulated by the Law of Georgia on Operative-Investigative Activities and were allowed only before launching an investigation.

215 The data published on the official webpage of the Supreme Court of Georgia does not contain information whether which agency was conducting the investigative action.

2016	401	315	30	56	Reviewed - 79 Upheld - 69 Upheld in part - 3 Denied - 7
2015	373	261	45	67	Reviewed - 85 Upheld - 72 Upheld in part - 9 Denied - 4
2014	1074	894	-	-	-

The amendments of the first of August of 2014 also defined the role of judiciary in the course of protection and destruction of data obtained through covert investigative activities. E.g.: materials obtained through covert investigative actions, that were found as inadmissible evidence by the court of law, will be immediately destroyed after the expire of 6 months following the delivery of the decision on the case by the court of final instance. Until destruction these materials will be stored in special storage facility of the court of law. The court also keeps the materials, obtained through covert investigative actions, that are added to case files as material evidence. The data/materials, obtained through covert investigative actions, are destroyed under the participation of a judge. A special report is draw up about the destruction of data/materials, obtained through covert investigative actions, which report is endorsed by the signatures of the prosecutor and the judge.[216]

Irrespective of legislative amendments wiretapping and the existing system of recording are materially deficient and are fraught with the jeopardy of violation of the right to privacy.[217] The so-called 'black box' (lawful interception management system), which ensures direct access to telephone conversations and content of communications transmitted through the Internet, is under the disposal of the State Security Service. The existence of this system ensures uncontrolled interception and storage of telecommunications data by the State Security Service in real time, without any oversight. Consequently, despite progressive legislative amendments, the existing system fails to ensure adequate protection, for wiretapping not to be done without judicial authorization. Holding of technical equipment by the State Security service and direct access to the content of communications involves increased risks of the abuse of power.[218]

4.2.2 JUDICIAL OVERSIGHT OF ELECTRONIC SURVEILLANCE

Apart from investigation purposes the State Security Service engages in secret surveillance and wiretapping within the framework of counterintelligence activities.

The State Security Service is entitled to deploy operative-technical measures[219] for counterintelligence purposes. Commensurate with the Law of Georgia on Counterintelligence Activities, judicial authorization is required only for electronic surveillance and control of mail correspondence.

According to law, the types of electronic surveillance are:

- Bugging and recording of telephone communication;
- Collection and recording of information from a telecommunications channel (through connection to telecommunications means, computer networks, linear communications and terminal equipment), computer system (both directly and remotely) and installation of relevant software into computer system to this end.

216 Code of Criminal Procedure of Georgia, Article 143[8].

217 "Nine threats to your personal life stemming from the new legislation on secret wiretapping," Transparency International - Georgia, 2014. http://www.transparency.ge/ge/content/stub-577.

218 Litigations on covert wiretapping case at the Constitutional Court. For details see Chapter 3.4 of the research.

219 Covert video and audio recording; covert filming and photography; use of telecameras and other electronic devices; electronic surveillance; control of mail correspondence; strategic monitoring; individual monitoring, determination of geolocation in real time.

A warrant of a Supreme Court judge is required to launch the electronic surveillance. The amendments, made to the Law on 22 March, 2017, introduced the institute of supervisor judge, who not only issues a warrant on launching electronic surveillance, but also supervises the process of enforcement of the measure in accordance with the procedure, prescribed by this Law.

The role of a supervising judge in the course of launching electronic surveillance - For electronic surveillance purposes an authorized representative of the Head of special service files a motion with the Supreme Court of Georgia. A judge will review the motion for authorization of the electronic surveillance not later, than within 24 hours after its receipt at a closed court session, under the participation of the authorized representative of the Head of special service. In the case of urgent necessity, when a delay may result in the destruction of important for the case factual data or render it impossible to obtain these data, the Head of special service is entitled to make a decision on launching electronic surveillance without a warrant of the supervising judge. In this case the authorized representative of the Head of special service is required to immediately notify the court of law about the foregoing and file a relevant motion within 24 hours after launching the electronic surveillance.

The role of a supervising judge in the course of electronic surveillance - a supervising judge is entitled to demand the submission of information about the flow of the electronic surveillance and data obtained through the electronic surveillance from special service; alto to suspend or terminate electronic surveillance in the case of existence of grounds prescribed by law.[220]

The role of a supervising judge in the course of destruction of data obtained through electronic surveillance - the data obtained through electronic surveillance, which is no more relevant for the fulfillment of the tasks of counterintelligence activities is destroyed by the authorized representative of the Head of special service in the presence of the supervising judge. A special report is drawn up on the destruction of this data, which is signed by the supervising judge and the authorized representative of the Head of special service.[221]

4.2.3 OTHER COVERT MEASURES, UNDERTAKEN BY SECURITY SERVICE WITHOUT JUDICIAL PARTICIPATION

Pursuant to the Law of Georgia on Counterintelligence Activities, the operative-technical measures, related to the restriction of constitutional rights and freedoms of natural and legal persons, are carried out on the basis of a court decision and in accordance with the procedure, prescribed by law.

Despite this stipulation no court authorization is required for measures (operational, operative-technical), carried out by the Security Service, that are closely linked with the restriction of the right to privacy, e.g. electronic surveillance (implemented under written consent of one of the parties to telephone or other type of electronic communication), infiltration of an undercover agent into a criminal group, strategic monitoring, individual monitoring. etc.

Particularly problematic is the conduct of covert audio and video recording, covert filming and photography and agreed electronic surveillance without judicial control. A constitutional claim concerning non-constitutionality of these measures is currently filed with and reviewed by the Constitutional Court of Georgia.[222]

According to the Law of Georgia on Counterintelligence Activities“ covert video and audio recording, filming and photography are operative-technical measures.[223]

220 Law of Georgia on Counterintelligence Activities, Article 14^4.

221 Law of Georgia on Counterintelligence Activities, Article 14^9.

222 One of the key arguments of claimants is launching and conduct of the operations concerned without judicial participation/ control. See the constitutional claim of Human Rights and Monitoring Centre (EMC) and Georgian nationals Guram Imnadze and Sophiko Berdzeuli against the Parliament of Georgia (Constitutional Claim N°690), https://goo.gl/ChX6qs.

223 Under Article 2(c) of the Law of Georgia on Counterintelligence Activities ‘operational-technical activity’ is a constituent part of counterintelligence activities including special measures, implemented through the application of special technical means, covert modes and methods, which aim at collecting information about intelligence or/and terrorist activities of special services, organizations, groups of persons and individual persons of foreign countries.

Although video and audio recording, filming and photography are measures restricting the right to privacy, the Law does not provide for grounds for their conduct, other than those, prescribed for other measures. The Law does not provide for the order, procedure of conduct and duration of covert recording, does not regulate the terms and conditions of storage and destruction of obtained data; owing to secret nature of the measure, the Law does not provide for any grounds for the verification of its legality. Consequently, covert recording, undertaken by Security Service for counterintelligence purposes, is carried out without any external, inter alia, judicial control.

Owing to particularly high degree of interference into personal life, these measures should be conducted under judicial authorization.

When State Security Service undertakes covert video, audio recording and photography for investigation purposes, the operation, as a covert investigative action, is subject to mandatory judicial control and is regulated by the Code of Criminal Procedure. If implemented within the framework of counterintelligence activities, the same operation does not require judicial authorization. Although the purpose of the operation is different, the type of action, nature of the operation and risks of willfulness and abuse of power are identical.

In the case of a covert operation an individual is not aware, that a right-restricting action is carried out against him and, respectively, is not in the position to apply to the court of law. Owing to the nature of the measure, the constitutional right of an individual of access to court is restricted and in this case the mechanism of prior judicial verification of a right-restricting action is the only legal guarantee for the protection of the right.[224]

Different standards for covert filming for investigation and counterintelligence purposes became particularly problematic when the Security Service was granted the right to conduct investigation. There is an increased jeopardy of willfulness and temptation that information obtained for analytical purposes to be used for the purposes of criminal investigation. The risk is further escalated by the fact, that there is no strict delimitation between the grounds of criminal persecution and data obtained through counterintelligence activities.

Commensurate with Paragraph 2 of Article 5 of the Law of Georgia on Counterintelligence Activities the main purpose of this activity is only the collection of information and it does not constitute ground for criminal persecution. Based on the forgoing the law tolerates the possibility that in certain cases information, obtained through counterintelligence activities may become grounds for criminal persecution despite the fact, that data, collected in such a manner cannot be admitted as evidence at the court of law.

The State Security Service is entitled to conduct electronic surveillance under written consent of one of the parties agreed electronic surveillance should not exceed 90 days.[225] In the case of agreed electronic surveillance the Law does not provide for the involvement of the court of law either in the initiation or conduct of the process. There are no external control mechanisms in the case of electronic surveillance either.

Prior written consent of one of the parties of a conversation cannot be offered as an alternative to a court authorization as it does not provide for adequate guarantees for the protection against willful and unreasonable restriction of this right. The person, against whom these actions are conducted covertly, under the consent of only one of the parties, is the victim of violation of right. The same concerns the procedure of interception and recording of information from telecommunications channels.

The disputed provision is simple way of evasion of judicial control as special services acquire the right to keep an eye on someone without judicial authorization, just under the consent of one of the parties to electronic communication. Covert obtaining of a message, received by telephone or other technical means, without judicial authorization contradicts Article 20 of the Constitution of Georgia, according to which Article the restriction of rights is allowed only under a court decision or without it, in the case of urgent necessity, envisaged by law.

---

224 In the Case *Leander v. Sweden* the ECHR stressed the necessity of legal guarantees in view of the risk that "a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it" (*Leander v. Sweden, Pragraph #60).* In the case of the *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* the Court found the violation of Article 8 of the Convention also in the fact, that court warrant covered only the stage before deployment of means of surveillance and no one verified whether these means in fact complied with the warrants authorizing the use of such means, there existed no independent review of whether the original data was in fact destroyed within the legal ten-day time-limit if the surveillance has proved fruitless (See *#62540/00.* Paragraph #85).

225 Law of Georgia on Counterintelligence Activities, Article 15.

4.2.4 THE BEST PRACTICE OF SELECTED COUNTRIES:

Supervision of judicial or quasi-judicial authorities over covert operations of security services.

Country	What does the court authorize?	What doesn't require authorization from the court	Expanding/terminating surveillance
Germany	• Use of secret surveillance activities • Foreign strategic secret surveillance	In emergency situations, surveillance measures can be implemented without G-10 commission's authorization, provided that retrospective authorization is sought without delay..	Targeted surveillance measures last for a maximum of 3 months, and extension is subjected to the same procedures. At any point of inspection, the commission can demand an immediate halt to the secret surveillance.
Canada	• Interception of any communications or obtaining any information, record, document or thing and, for that purpose • (i) entering any place or obtaining access to anything, • (II) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing • (III) to install, maintain or remove anything		Renewal of warrants are also subjected to double approval by Minister responsible for CSIS and the federal court judge
Croatia	• surveillance of the communication content • surveillance of posts • surveillance of facilities and closed spaces • audio recording of communications between persons in open and public spaces	• Surveillance of telecommunication traffic data • Surveillance of the location of the user (a and b indicating metadata) • Surveillance of international telecommunications • Secret purchase of documents and objects	Extensions are authorized by a panel composed of three authorized judges of the Supreme Court

Belgium	• Hacking into electronic systems • The use of human agents including through the creation of false identities • Observation in and searches of private dwellings	• inspecting identification data • localisation and call-associated data of electronic communications • Cooperation of a communications operator	

4.2.5 SUMMARY AND RECOMMENDATIONS

Judicial control of covert measures conducted by Security Service is an important guarantee in view of protection of the right to privacy. As evidenced by the best international practice, the court oversees not only launching the covert measures, but also their conduct. And in countries, where the court of law does not issue a warrant to conduct covert measures, there are the other efficient mechanisms of external control in place.

Despite recent positive changes made to Georgian law, a number of covert measures are still beyond judicial control, which measures are marked with intensive interference into personal life. These measures are not subject to other mechanisms of external control either and respectively the risk of the abuse of power and violation of the right to privacy is rather high.

The current system of secret surveillance and wiretapping - ownership of technical equipment by the legal entity of public law under the subordination of the State Security Service and direct uncontrolled access to information about the communications of the citizens involves the high risk of the abuse of power and contradicts the Decision of the Constitutional Court of Georgia of 14 April, 2016.

With a view to protection of human rights in the course of conduct of covert measures by Security Service, alignment of the legislation with international standards and the Constitution of Georgia it is reasonable to make the following changes and amendments to legal framework:

- Technical means (including software) allowing for the collection of personal information in real time should be created, owned, administered and direct access to personal information through these means should be enjoyed, also identification data (metadata) should be copied and stored by such independent agency, which is not vested with an investigative function or is not professionally interested in reviewing this information. LEPL - Material-Technical Agency, a subordinated to the State Security Service authority, does not meet these requirements.
- Judicial control should be extended to covert video and audio recording, covert filming and photography for counterintelligence purposes, the judiciary should be involved not only at the stage of issuance of an authorization, but also it should inspect the conduct of such measures and destruction of obtained data;
- Judicial control should be extended to agreed electronic surveillance as restriction of the right to privacy of the person who is wiretapped, is as intensive as in the case of electronic surveillance;
- In the case of other covert measures, which are not subject to judicial control, the efficient mechanisms of external control should apply to protection of personal data in the course of conduct of these measure (e.g. submission of information to a special Parliamentary committee, oversight expert board, Personal Data Protection Inspector, etc.)

4.3 OVERSIGHT OF STATE SECURITY SERVICES BY INDEPENDENT AGENCIES

4.3.1 OVERSIGHT OF STATE AUDIT SERVICE OVER THE EXPENDITURE OF PUBLIC FUNDS BY STATE SECURITY SERVICE

The analysis of international practice allows for identification of several main reasons conditioning particular importance of financial oversight of security services, amongst them:

- Provision of insights into the behavior and performance of the Service through financial records;
- Limited scope of public control due to secret nature of the Service activities;
- Financial risks, including the risk of the misuse of public funds.[226]

The above reasons and specific nature of behavior and performance of security services condition the existence of special methods and institutions for efficient oversight thereof.

The Parliament oversees the disbursement of public funds in State Security Service through State Audit Service as well. Important lever of oversight over the control of financial expenditures of the State Security Service is the Trust Group of the Parliament of Georgia.[227]

The function of the Audit Service to oversee the expenditure of public funds is prescribed by the Constitution. The Constitution provides for the guarantees of independence of the Audit Service and its accountability only to the Parliament. The independence of the Audit Service is also guaranteed by the election of the Auditor General for a definite term and his/her dismissal through impeachment procedure.[228]

According to the Law of Georgia on State Security Service "The utilization and disbursement of the resources of the state budget of Georgia and other material values by the Service State is overseen by the State Audit Service." The oversight of the State Audit Service extends to programs of every level funded from the state budget,[229] and the oversight is accomplished by the Audit Service through instruments, prescribed by law. The key instruments are the reports on the fulfillment of the state budget by the Government and the conduct of various types of audit (financial, compatibility, efficiency).

The Government submits an Annual Report on the Fulfillment of the State Budget to the Audit Service before the first of April of each ear,[230] and the State Audit Service submits a Summary Report to the Parliament on Annual Report on the Fulfillment of the State Budget within a period of 45 days.[231]

Apart from annual reports the Audit Service prepares a Summary Report on the Report on Fulfillment of the Budget of the Current Year, which is submitted to the Parliament during the review to the draft budget. The Parliaments reviews the Summary Report of the Audit Service together with the Report on the Fulfillment of the Budget. It is reviewed by Parliamentary committees, factions, majority, and the minority. The process ends up with the review of the Summary Report and the Report, as a result of what the Parliaments votes for the fulfillment of the Budget.[232]

From the date of creation of the State Security Service - the first of August, 2015 - up to the end of 2017 the Audit Service presented its Summary Reports on three current (2015-2017) and two annual (201, 2016) reports on the fulfillment of the budget.[233]

---

226 Born and Willis , 2012, p. 213.

227 For details see the Chapter on Parliamentary Oversight.

228 Ibid, Article 64 and Paragraph 2 of Article 97.

229 According to Article 15 of the Law of Georgia on the State Budget of Georgia for 2018 the assignments for State Security Service (classification Code 20 00) in 2018 amount to 124 million GEL.

230 Budgetary Code of Georgia, Article 55, Paragraph 1.

231 Budgetary Code of Georgia, Article 31, Paragraph 1.

232 Rules of Procedure of the Parliament of Georgia, Article 190.

233 According to their essence the Reports of the State Audit Service are apolitical papers, where the fulfillment of the budget is evaluated only according to criteria, set by law, they also rely on the reports of the State Treasury on the fulfillment of the Budget, reports of the National Bank, reports of expending agencies, data of National Statistics Office, also the outcomes of the audit inspections, carried out by the Audit Service itself, etc. (See e.g.: Summary Report on Annual Report on the Fulfillment of the State Budget of 2016, Full List of Reference Materials, p.5 available athttps://sao.ge/files/auditi/moxseneba-2016-biujetis-shesrulebis-cliuri-

The State Security Service is not mentioned in Summary Reports on the Report on Current Fulfillment of the Budget, while the Annual Reports on Fulfillment of the Budget highlights certain financial deficiencies:

It is stated in Summary Report on Annual Report on the Fulfillment of the State Budget of 2015[234] that Central Office, Counterintelligence Department and State Security Department of the State Security Service of Georgia have rather low showings of budgetary funds disbursed during a year as compared with the plan approved at the beginning of the year.[235] When analyzing the management, accounting and reporting on state funds in budgetary organizations the same Summary Report says that despite the improvement of the situation in this field as a result of reform, there still are essential shortcomings. "Specifically, in most cases the financial statements of expending agencies do not provide true and fair picture of their financial standing. Furthermore, there are the cases of violation of regulatory rules in the course of accounting and reporting, what, in its turn, speaks for the weak points of internal control."[236] As an example of this shortcoming the Summary Report, inter alia, refers to the case when nonfinancial assets (32 buildings) and land plots were not put on the books of the State Security Service as a result of separation of the State Security Service from the Ministry of Internal Affairs.[237]

It is stated in the Summary Report on Annual Report on the Fulfillment of the State Budget of 2016,[238] that 1,399,710 and 3,999,987 GEL were allocated from the reserve fund of the Government for the State Security Service in 2015 and 2016. The purpose of allocation of the funds reads to be: "For smooth operation of the State Security Service of Georgia."[239] The Summary Report says, that funding allocated on similar grounds, without a specific reason „leaves in serious doubt the necessity of funding of these expenses from the resources of the reserve fund.[240] It is further explained, that according the Budgetary Code only those payments are funded from the reserve fund, which cannot be taken into account for objective reasons while planning the budget, and in the case concerned, like previous years "the resources are allocated for funding such expenses, which are of systematic nature and in the case of proper planning, they could have been accounted for in the assignments of respective expending agencies at budget planning stage."

The analysis of both Summary Reports evidences, that the State Security Service had problems with the disbursement of the budget in 2015, however, despite the foregoing, 1,399,710 GEL were still allocated for the agency in 2016 from the reserve fund of the Government "For smooth operation". This situation is not mentioned in the Report of the Audit Service.

Hence, for two years of existence of the State Security Service the Audit Service has not reported about problems within the State Security Service to the Parliament within the framework of oversight of the fulfillment of the Budget. The Audit Service exercised only ex-post oversight over the fulfillment of the budget by the State Security Service and described only those problems, the part of which could have been highlighted in interim report as well.

Conduct of audit inspections at budgetary organizations is the main procedure of work of the State Audit Service. By the end of each year the State Audit Service makes a annual plan of audit activities, where the budgetary organizations, where the audit will be held the next year, are defined. The Audit Service is independent in making the plan[241] and is limited only by the methodology, drafted thereby.[242]

Using this methodology total 183 audits were planned in 2016-2017, however, the State Security Service was not amongst agencies, subject to audit. 102 audits are planned for 2018 and the State Security Service is

---

angarishis-shesaxeb.pdf.)

234 Summary Report on Annual Report on the Fulfillment of the State Budget of 2015, available at: https://info.parliament.ge/#law-drafting/12015.

235 Ibid, p. 88.

236 Ibid, p. 229.

237 For further details see ibid, p. 232.

238 Summary Report on Annual Report on the Fulfillment of the State Budget of 2016, available at: https://info.parliament.ge/#law-drafting/13878.

239 The purpose of 24% of resources, disbursed from the reserve fund of the Government in 2016 was smooth operation of the agencies and funding their current needs. See ibid p.172.

240 Ibid.

241 Law of Georgia on State Audit, Article 17, Para. 3.

242 Para. 3 of Article 227 of the Rules of Procedure of the Parliament obliges the State Audit Service to take account of the proposals of the Parliamentary committees, investigative and other temporary commissions upon drafting its action plan.

again not on the list. Making the annual plan of audits is the sole prerogative of the Audit Service, however the methodology of its drafting allows for accounting for the factors, like high risk and public interest. [243] The Audit Service defines priority areas on the basis of these factors. [244] The State Security Service should be considered as a high risk expending agency due to several reasons: no audit inspection has ever been carried out therein and specific nature of its activities inherently implies limited transparency. Respectively, the role of Audit Service is of crucial importance in exercising oversight thereon.

Of particular importance is the audit inspection of budgetary organizations, where secret information is held. E.g. owing to secret nature of data additional risks are proved in the Financial Audit Report of the Office of the Ministry of Internal Affairs of Georgia of 2016: *"The randomized inspection of agreements marked "top-secret" revealed, that some of them (approximately 5% of net contract value) contained no secret information and they failed to present any relevant justification either. Hence, we, the members of the Audit group have not assured ourselves of the legality of classification of these documents."* [245] The foregoing situation is an apparent example of non-targeted classification of information and it is also evident that there is a risk of similar violation in the State Security Service as well. In this case the only means of oversight is for the Audit Service to carrying out the audit inspection.

Furthermore, it is important that the Service needs access to classified information for the conduct of comprehensive inspection at the State Security Service. The Auditor General is automatically vested with such access upon his/her election by the Parliament,[246] as regards the personnel of the Audit service, the law required for them to undergo special procedure to gain access to classified information, which access is granted to an individual or to a legal entity/organization and the procedure is conducted by the State Security Service.[247] In the case of Audit Service will be reviewed in every 5 years.

4.3.2 THE ROLE OF THE PUBLIC DEFENDER IN THE OVERSIGHT OF THE STATE SECURITY SERVICE

Amongst independent institutions, overseeing the State Security Service, the institute of Public Defenders holds a key position.

Georgian law empowers the Public Defender with all relevant rights concurrent with Paris Principles, what is proved by the fact, that it is awarded with "A" status by the Global Alliance of National Human Rights Institutions (GAHIRI). This status is awarded as a result of accreditation procedure, conducted under the UN aegis and certifies full compliance of the Office of Public Defender with Paris Principles.[248]

According to international practice the mandate of Ombudsman's institutes extends to all governmental agencies, including security services. In Georgia the Public Defender does not enjoy any special powers with regard to State Security Service and exercises the oversight according to general rules.

In countries like Georgia, where there are no expert authorities to oversee security services, the role of the institute of Ombudsman is particularly important, amongst them with regard to review of complaints and visual inspection of the institutions. The review of complaints and statements is one of the key powers of the Public Defender. Below it is described, whether what kind of complaints are subject to review of the Public Defender.

The guarantees granted to Public Defender by law allows the latter to have access to data held by the State Security Service, what is important precondition of oversight. The Public Defender is granted access to state classified information as soon as he/she is appointed.[249] Furthermore, the Public Defender is entitled to freely enter any state or local government authority, request documents, explanations necessary for their

243 See The Methodology of Drafting Annual Plan of Audit Activities, p. 3.

244 Priorities of Audit Service: https://sao.ge/audit/audit-planning-process/sao-s-priorities

245 Summary Report on Financial Audit of the Office of the Ministry of Internal Affairs (30 01 01 01) of 2016 , 2017, p. 35, available at: https://sao.ge/files/auditi/auditis-angarishebi/2017/saq+SHss.pdf.

246 Law of Georgia on State Secrecy, Article 18.

247 Ibid, Article 20.

248 CHART OF THE STATUS OF NATIONAL INSTITUTIONS, accreditation status as of 26 May 2017, p. 7, available at: http://www.ohchr.org/Documents/Countries/NHRI/Chart_Status_NIs.pdf

249 Law of Georgia on State Secrecy, Article 18.

inspection, conduct expertise with the help of invited experts, etc.[250]

For the exercise of these powers and evaluation of the situation in the country with regard to human rights and freedoms the Public Defender investigates violations both on the grounds of complaints and on his/her own initiative.[251]

For state security oversight purposes, particularly pressing is the power of the Ombudsman to examine the compatibility of a normative act with Chapter 2 of the Constitution of Georgia on the basis of a complaint, as important internal acts of the Security Service are classified as containing state secrecy. However, it is extremely important for the Public Defender to have the same authorization without a complaint and be able to examine these acts on his/her own initiative. It is possible for this power to be discernible from the current version of the Organic Law of Georgia on Public Defender,[252] however it is important for the Law to contain specific stipulation and such practice of inspection to be intensively deployed.

The Public Defender's reaction to violations are mainly of recommendatory nature.[253] They are fully listed in Article 21 of the Law, of which the relevant for the oversight of the State Security Service instruments can be identified:

- To send proposals and recommendations for the restitution of violated human rights and freedoms to the authority, whose actions caused the violation of the right;
- To request launching an investigation and/or criminal prosecution from relevant investigating authorities if, after examining the case, he/she arrives to the conclusion that there are the elements of a crime;
- To make proposals to relevant bodies regarding disciplinary or administrative liability of persons whose actions caused a violation of human rights and freedoms;
- inform the mass-media about the results of the inspections held with regard to violations of human rights and freedoms;
- To include decisions made thereby into annual and special reports;
- To apply to the courts of law in the capacity of a friend of the court (Amicus Curiae);
- To apply to the Parliament of Georgia in urgent cases and request setting up a temporary investigation commission with regard to violation of human rights and freedoms and review of these issues by the Parliament;
- To apply in writing to the President of Georgia, the Prime-Minister of Georgia, if the Public Defender of Georgia considers that the remedies at the disposal thereof are not sufficient.

In countries, where there are bodies exercising oversight over the state security service, comprised of independent experts, the Public Defender closely cooperates with them. Worth mentioning is Belgian practice, were the key function of the Ombudsman is the assessment of the complaints related to state security service and pre-selection of relevant petitions from those that are deemed irrelevant, of minor importance and groundless and transmission of well-grounded complaints to the Committee I, which is responsible to their review.[254] Committee I is an independent expert body, set up by the Parliament, supervising the security service. Such cooperation between oversight authorities aims and further improvement of the accountability system efficiency.

Within the framework of the survey we have requested information from the Office of the Public Defender about oversight measures undertaken thereby with regard to State Security Service.[255] According to provided information, during the reporting period most of the alleged violations of human rights, recorded by the Public Defender, concerned the questions of granting the right of residence and citizenship. With respect to granting the right of residence the Public Defender receives individual applications, following the

250 Organic Law of Georgia on Public Defender of Georgia, Article 18.

251 Ibid, Article 12.

252 The foregoing stems from systemic interpretation of Para. 1(d) of Article 14 of Law with Article 12..

253 Except for application to the Constitutional Court.

254 EU FRA Surveillance by Intelligence Services Vol. 2 (2017), p.132.

255 Requested information #03-4514.

scrutiny of which the recommendations are issued in the case if the violation of human rights is established. E.g. in the Parliamentary Report 2015 the Ombudsman issued the following recommendation to the State Security Service with regard to issuance of residence permits:

„In the case of issuance of a negative opinion with regard to granting residence permit and citizenship for national or/and public security reasons, concurrent with statutory requirements justification should be ensured, specifically, reference to specific grounds (subparagraph) and provision of adequate information to persons, whose requests were denied."[256]

In the Report 2016 the above recommendation is just copied without any changes, meaning that the problem was still topical and the recommendation - not fulfilled.[257]

The next issue discussed by the Public Defender in his Reports with regard to the State Security Service concerned the so-called "ODRs" (Russian abbreviation that stands for "Active Reserve Officer)". In his Report 2015 the Ombudsman called the Parliament to "set up a temporary investigation commission to study future application of the institute of "ODRs" after the amendments made to the Law, amongst them at the institutions, where their deployment was excluded by law".[258] This recommendation was not upheld by the Parliament.

The case of 2016 should be reviewed in the light of oversight power of the Ombudsman, when allegedly ill-treatment of a person detained by the State Security Service for charges in terrorism became the object of Public Defender's scrutiny.[259]

The mention should be made of Public Defender's intensive efforts with regard to recognition of the system of wiretapping unconstitutional. In 2016 the Constitutional Court of Georgia upheld the action of Public Defender together with the action of the organizations participating in the campaign "This Concerns You" and found the existing system of secret surveillance unconstitutional. In 2017 the Public Defender again applied to the Constitutional Court as the Law, adopted by the Parliament - under which law the secret surveillance is performed by Operative-Technical Agency - contradicts the Decision of the Constitutional Court of Georgia. The Case is still pending at the Constitutional Court of Georgia.[260]

Based on the last two Annual Reports of the Public Defender it can be said that the Public Defender's oversight of the State Security Service was mainly focused on the criticism of the practice of the so-called "ODRs" and violation of human rights upon granting residence permits to foreign nationals. Also the Public Defender played an important role in appealing the system of secret surveillance with the Constitutional Court and review of the issue.

256 The Situation with Regard to Human Rights and Freedoms in Georgia, Report of the Public Defender, 2015, p. 864.

257 The Situation with Regard to Human Rights and Freedoms in Georgia, Report of the Public Defender, 2016, p. 796.

258 The Situation with Regard to Human Rights and Freedoms in Georgia, Report of the Public Defender, 2015, p. 8.

259 See Public Defender's Statement of 23 August, 2016, on Alleged Ill-Treatment of Beka Bekauri, Who Is Charged with Terrorism.

260 For details see Chapter 3.3.1

* Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.12

Country	Powers of the Ombudsman
Croatia	Right to launch investigation into human rights violation by the Security Service. The Ombudsman (as well as the deputy) doesn't need special security clearance to gain access to classified information.*
Belgium	Due to the functioning of two strong expert oversight bodies, the Ombudsman has a secondary role in oversight. The Ombudsman has a mandate to receive and review complaints, to assess and filter out irrelevant complaints. The Ombudsmand sends only substantiated complaints to the Committee I, which is responsible for its review.
Canada	The mandate of Canada's Human Right's Commission covers all federal bodies, including the power to review complaints lodged against the Security Service. During the review, the law gives the SIRC (Security Intelligence Oversight Committee) the right to work jointly with the Human Rights Commission, which is an example of best practice. On the regional level, the Ombudsman institutions are also active in protecting right to private life and personal data, as well as raising awareness on issues related to the transparency of the government bodies.*
Germany	An ombudsman institution doesn't function on the federal level in Germany. However, the Parliamentary Complaints Commission fulfills the function of the ombudsman and receives complaints lodged against all federal agencies. As in the case of the Belgian Ombudsman, the Complaints Commission filters the complaints and sends substantiated complaints to the parliamentary control group. The Group has the power to independently investigate the complaint or send it to the G-10 Commission, especially if the issue requires technical knowledge.**

4.3.3 OVERSIGHT OF THE USE AND PROTECTION OF PERSONAL DATA BY THE SECURITY SERVICE

The oversight of protection of personal data in Georgia is accomplished by Personal Data Protection Inspector.[261]

The topicality, as well as complexity of protection of personal data in security sector are associated with the mandate of the Service itself and classified nature of its activities. For comprehensive oversight a controlling authority should have the relevant competence, human and material resources and full access to state secrecy whereas the absolute majority of the activities of the State Security Service are classified.

The mandate of Personal Data Protection Inspector extends to all public and private entities, *inter alia*, to the procession of personal data by the Security Service. However, limited access of Personal Data Protection Inspector to information classified as state secrecy, makes it impossible for the Inspector to exercise comprehensive oversight of the State Security Service.

There is no other agency either to oversee the procession of personal data classified as state secrecy for state security, defense, intelligence and counterintelligence purposes. Consequently, there exists no external control mechanism.

There is no uniform standard of protection of personal data within security system in the EU Member States. According to international practice, oversight of protection of personal data by security services is accomplished by several actors. Every European country has personal data protection agencies (DPA), which in specific cases assume the duty to inspect the administrative buildings and documents of the security services.[262]

In some European countries a parliamentary committee or an expert oversight body is delegated with the mandate to oversee the use, storage and transfer of personal data by security services.[263] There exists the practice of intensive cooperation between independent expert boards and personal data protection special agencies. E.g. in Croatia, Council for Civilian Oversight of Security and Intelligence Services and Personal Data Protection Agency of Croatia exercise oversight of covert operations through initiation of investigations, targeted inquests on complaints or on-sight physical inspection. Decisions of Personal Data Protection Agency of Croatia are of binding nature.[264]
No matter which body oversees the protection of personal data in security sector, the best practice according to the UN guideline is the deletion of any such information to be supervised by an external institution.[265]

Personal Data Protection Inspector oversees the legality of data protection in Georgia in several directions and through several means, amongst them, through the inspection of the legality of data procession at public and private institutions.[266]

The Inspector is entitled to enter any institution or organization for inspection purposes and review any document and data, amongst them, the data containing commercial or professional secrecy, also the materials of operational-search activities and crime investigation, classified as state secrecy, irrespective of their contents and storage mode. Regardless of the above stipulation, the Law provides for a restriction, what makes impossible for Personal Data Protection Inspector to comprehensively oversee the State Security Service. In particular, commensurate with the Law of Georgia on Personal Data Protection "the Law does not apply to the procession of data classified as state secrecy for state security (inter alia, economic

---

* See for instance the Manitoba Ombudsman. http://www.theioi.org/ioi-news/current-news/ombudsman-celebrates-right-to-know-week

** German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.21.

261 The Parliament of Georgia adopted the Law on Personal Data Protection in 2012, and the Personal Data Protection Inspector was elected in 2013.

262 Mandate and powers of DPAs in the EU vary. Some countries entrust DPAs with powers to oversee security services, others exclude security services from the mandate of DPAs. See *EU FRA, Surveillance by Intelligence Services (2015), p.50.*

263 See Chapter 3.1.1.3.

264 See *EU FRA Surveillance by Intelligence Services, Vol. 2. (2017), p.115.*

265 UN Compilation of Good Practices, Practices 24-25.

266 The other duties of the Inspector are: provision of advise to public and private institutions and natural person on various aspects of data protection, review of applications related to data protection, provision of information to the society at large about the situation in Georgia with regard to data protection and related thereto important events.

security), defense, intelligence and counterintelligence purposes."[267] Respectively, on the one hand, the Inspector is entitled to inspect the State Security Service, but on the other - the Inspector's mandate is limited with regard to procession of data classified as state secrecy, where the risk of violation of personal data is particularly high.

By virtue of amendments made to the Law of Georgia on Personal Data protection in 2014, the Inspector was granted the right to oversee the process of initiation of wiretapping and copying identification data from databases using the electronic system of control. According to the Law a operation could have been launched only after technical authorization of launching wiretapping process by the Inspector.[268] However, technical equipment used for wiretapping is owned by the LEPL - Operative-Technical Agency, operating within the framework of the State Security Service[269] and the Inspector oversees the wiretapping process through the system, which was created by the State Security Service itself. Consequently, the Inspector is not in the position to minimize the risk of the abuse of power and to exclude the possibility of wiretapping by the Security Service without the authorization of the Inspector.[270] It should be mentioned that the Inspector enjoys the right to technically authorize wiretapping only during covert investigative actions. The Inspector is not in the position to oversee the electronic surveillance for counterintelligence purposes.
According to legislative amendments of March 2017 prior authorization of the Inspector is no more required for launching wiretapping and recording a telephone communication. The LEPL - Operative-Technical Agency acquires the right to launch this investigative action just in the case of confirmation of the provision of the electronic versions of the ruling and resolution to the Inspector via the special program. According to Law the Office of the Inspector continuously oversees the ongoing process. The Personal Data Protection Inspector was granted the right to suspend wiretapping and recording a telephone communication if no electronic or hard copy of a ruling of a judge or resolution of a prosecutor is presented to the Office, or when the electronic and hard copies of prosecutor's resolution do not coincide or/and there is some ambiguity/inaccuracy therein.

Another important power of the Inspector is the right to inspect the LEPL - Operative-Technical Agency of the State Security Service, when the Inspector is entitled:

- To enter the limited access areas of the Agency and observe the ongoing activities of the authorized bodies;
- To review the regulatory legal documents (inculing ones, containig state secrecy) and technical guidelines of the Agency;
- To receive information about technical infrastructure used for the purposes of covert investigative activities and inspect this infrastructure;
- Demand explanations from Agency personnel with regard to specific issues, revealed during the inspection.[271]

The information about the oversight of the State Security Service, exercised by Personal Data Protection Inspector within the scope of his mandate is contained in the Annual Report on the State of Personal Data Protection and Activities of the Inspector.

According to provided information Personal Data Protection Inspector gave 6 recommendations and 5 assignments to the State Security Service in 2016-2017. The Service ensured the fulfillment of both the recommendations and the assignments.

Personal Data Protection Inspector received three applications from three citizens regarding allegedly unlawful procession of data by the Security Service. The applications of two citizens are already reviewed and no breach of law has been revealed. The review of the third application is still pending.

The Annual Reports of Personal Data Protection Inspector mainly focus on interception of telephone conversations, however only within the framework of covert investigative activities, whereas, as already

267 Law of Georgia on Personal Data Protection, Article 3, Para. 3(c).

268 Law of Georgia on Personal Data Protection, Article 35[1].

269 The Agency undertakes wiretapping not only for the State Security Service, but also all those state authorities, who are vested with investigative authority and, respectively, undertake covert investigative actions.

270 For details of the existing system of wiretapping see Chapter 3.3.1.

271 Law of Georgia on Personal Data Protection, Article 35[1], Para. 4[1].

mentioned, Inspector's oversight mandate does not apply to electronic surveillance (interception of telephone communications and collection of information from the Internet) carried out for counterintelligence purposes.

According to Annual Report on the State of Personal Data Protection and Activities - 2015 of the Inspector, certain discrepancies were found in few court rulings on covert investigative activities in 2014-2015. In particular, in some cases court rulings did not include time limits for covert investigative activities or there was discrepancy in the data of the subject of covert investigative operation or those of the implementing agency. In the case of prolongation of the time limit of covert investigative operation, specific deadline was not indicated.

As per the data for 9 months of 2015, due to the above reasons, the Inspector's authorization was not granted not on opening the channel and wiretapping on average in four cases per month.[272]

As per Annual Report 2016, the number of court rulings submitted to the Inspector's Office has increased by 28, as compared to the previous year, while the number of motions for the extension of the term has decreased by 6 in 2016.

In 2016 the Inspector did not to grant authorization through the two-stage electronic system of covert investigative activities in 47 cases due to technical errors detected during the examination of the legality of grounds for data procession or inaccuracies/ambiguities in the resolution part of the ruling. Authorization was granted when these inaccuracies were addressed. It was also stressed in this Report, that in 2016 the inspection of the Operative-Technical Unit of the State Security Service was completed, which aimed at the examination of the legality of covert investigative activities (interception of telephone conversations and collection of information from the Internet) and activities concerning data banks. [273]

The inspection revealed various deficiencies concerning procedural, technical and legal aspects of covert investigative activities and activities carried out in data banks. By decision of the Inspector, the State Security Service was given certain recommendations/assignments and special timelines were set for their fulfillment. Commensurate with the decision of the Inspector the Operative-Technical Department of the State Security Service presented information about the fulfillment of issued recommendations/assignments in dues course.[274]

According to Annual Report 2017[275] the Inspector's Office did not grant authorization for covert investigative action through two-stage electronic system in 4 cases under the law in force before March 31, 2017. Since April 2017 the suspension mechanism was deployed with regard to 21 rulings/resolutions. The covert investigative activities continued after the elimination of the grounds of suspension.[276]

As per the Report the Personal Data Protection Inspector investigated the legality of data procession by the State Security Service and LEPL - Operative-Technical Agency in 5 cases.[277]

Against the applications of the citizens the Inspector examined the lawfulness of provision of information to data subjects by the State security Service of Georgia. As a result the cases of delayed or/and incomplete provision of requested information to data subjects were revealed.

According to Annual Report of the Personal Data Protection Inspector two inspections were carried out in 2017 with a view to examining the lawfulness of data processing conducted by the LEPL - Operative-Technical Agency in the course of wiretapping for the purposes of investigation. According to Annual

272 Annual Report on the State of Personal Data Protection and Activities of the Inspector - 2015 https://goo.gl/VczSDx, p.37

273 The inspection started in November 2015.

274 Annual Report on the State of Personal Data Protection and Activities of the Inspector - 2016, https://goo.gl/VczSDx, p. 64.

275 Annual Report on the State of Personal Data Protection and Activities of the Inspector - 2017 https://personaldata.ge/manage/res/images/2018/angarishi/angarishi_2017.pdf

276 According to Inspector's Report the number of motions on retrieval and recording of information from communication channels has decreased compared to the previous years. In addition, the number of prosecutor's resolutions submitted to the Inspector requesting initiation of investigative activity to collect computer data due to urgent necessity has decreased and computer data is usually obtained based on a court ruling.

277 In 2017, within the framework of inspection the Inspector investigated the legality of procession of data by law enforcement agencies for various reasons in 77 cases.

Reports of the State Security Service, the Agency was thrice inspected in 2017.[278] Furthermore, the joint inspection of the Chief Prosecutor's Office of Georgia and the State Security Service of Georgia was also conducted in 2017, which inspection aimed at the examination of the lawfulness of procession of the data of several persons/data subjects through covert investigative actions. The inspection did not reveal the commitment of the violation, envisaged by the Law of Georgia on Personal Data Protection by the Chief Prosecutor's Office of Georgia, State Security Service of Georgia and the LEPL Operative-Technical Agency.

The Annual Report of Personal Data Protection Inspector for 2 past years pay particular attention to the performance of covert investigative actions by the State Security Service and insofar as the Inspector has no access to other information held by the Security Service owing to the scope of Inspector's access to classified information. The Reports of the Inspector clearly evidence, that personal data protection will remain beyond the oversight unless a special institution is created (which, according to international practice, is an oversight board of the Parliament), which will have full access to information held by the Security Service.

Acting within the scope of his mandate the Personal Data Protection Inspector oversees the protection of personal data at the State Security Service and reviews the complaints of the citizens. However, the oversight does not extend to the protection of data classified as state secrecy for the purposes of state security (including economic security), defense, intelligence and counterintelligence activities.

In most cases the operations of the Security Service constitute state secrecy for security reasons. And the risk of violation of rights in the course of data protection is particularly high during covert operations. In the case of covert operations the oversight should cover the following directions: whether or not the personal data are obtained lawfully (authorization of the court of law or other external authorities), whether or not the personal data are obtained pro rata to a legitimate purpose, whether or not the security services are undertaking necessary measures to ensure the protection of data against their usage and disclosure for purposes, outside the mandate of the oversight body, whether or not the personal data, which are not/no more necessary for the legitimate purposes of security, are destroyed in accordance with the frame, prescribed by law.

4.3.4 SUMMARY AND RECOMMENDATIONS

The scope of oversight of the State Security Service by independent institutions is of paramount importance. The expenditure of secret funds by the Security Service, the volume of personal data accumulated within the Service and abundance of covert operations make particularly pressing the efficient oversight of the Service by independent, politically neutral institutions.

A serious challenge is the oversight of personal data protection within the State Security Service. The limited mandate of Personal Data Protection Inspector, what is conditioned by banning him from the access to classified information in security field, renders impossible the latter's oversight of the State Security Service. And what is more, no other agency has the mandate to oversee the personal data protection within the State Security Service.
For the oversight to be efficient it is important for an oversight authority to have full access to state secrecy, for the oversight to be intensive and the coordination between oversight authorities to be tight.

To intensify the oversight of independent controlling authorities over the State Security Service it is reasonable:

- To extend the oversight of personal data protection to covert operations of the Security Service as well. According to the best international practice in this field, this function should be exercised by the Parliament, and more specifically, by an independent board for the oversight of security sector.
- For the State Audit Service to set priorities of its audit activities so as to make it possible to efficiently oversee the expending institutions having secret funds, inter alia, the State Security Service.
- For the Public Defender to inspect the compatibility of the secret normative acts of the State Security Service with human rights standards on his/her own initiative, without the applications/complaints of the citizens and provide the Service with relevant recommendations. The Public Defender should be granted authority to raise questions with the Parliamentary supervisory board overseeing the State Security Service.

278 State Security Service Annual Report 2017 https://info.parliament.ge/file/1/BillReviewContent/179498 p. 20.

4.4. INTERNAL CONTROL OF THE SECURITY SERVICE

For adequate oversight of security services it is important for internal control to be in place along with efficient external control, and it should be continuously exercised over the activities of the Service. It is necessary to assess the existing mechanism of internal control on the one hand and on the other - external oversight of the practice and policy of its implementation.

Internal control of the State Security Service of Georgia is exercised by the General Inspectorate, whose powers and operational procedures are regulated both by the Law of Georgia on State Security Service and the Regulations of the General Inspectorate,[279] which is drafted on the basis of the Regulations of the General Inspectorate of the Ministry of Internal Affairs of Georgia and only a few, inherent for the State Security Service, specific amendments are made thereto.

The Law and the Regulations impose the following tasks on the General Inspectorate:

- Oversight of the observance of legal requirements within the State Security Service System;
- Revealing and adequate addressing of unlawful actions, violation of disciplinary rules, mal-performance of official duties;
- Provision of recommendations to the Head of the State Security Service with a view to revealing/ prevention/removal of the reasons promoting the violation of law;
- Revealing the cases of the conflict of interests;
- Revealing potential channels of unlawful disclosure of state secrecy and/or other official information;
- Conduct of procedural activities with regard to cases referred thereto by the Chief Prosecutor for investigation.[280]

The powers of the Inspectorate extends to structural subdivisions and territorial bodies of the Service, also to legal entities of public law operating within the framework of the Service.

The independence of the Service is declared by law, however the Head of the Inspectorate is fully subordinated to the Head of the Service, who appoints to and removes the former from the office, Furthermore the Head of Inspectorate is accountable to the Head of the Service and submits reports thereto on an annual basis or on request. Full dependence of the Head of the Inspectorate on the Head of the Service generates a risk of unauthorized influence of the Head of the State Security Service over the activities of the Inspectorate, informal interference into disciplinary proceedings that may aim at influencing a specific officer or attaining some other non-conventional purpose.[281]

According to Regulations the Inspectorate can conduct an internal inspection on several basis:

- Information about a violation and disciplinary misconduct committed by a Service officer obtained from the statements, complaints and reports of the citizens ot Service officers;
- Private rulings (decrees) of the court of law (judge);
- Notices and materials received from state authorities and administrative bodies, also from legal or natural persons, information disseminated through mass-media.

Although the Regulations also provides for notices, received from citizens, as grounds for initiation of internal inspection, the efficient form of citizens' application to the Inspection is not practiced, unlike the Ministry of Internal Affairs of Georgia.[282] However, like the Ministry of Internal Affairs, the State Security Service is conducting investigations, envisaged by procedure law, with regard to certain articles of the Criminal Code, on a systematic and routine basis what naturally implies the permanent risk of violation of rights.

279 Order of the Head of the State Security Service of Georgia N°8 of the first of August, 2015 On Approval of the Regulations of the General Inspectorate (Department) of the State Security Service of Georgia.

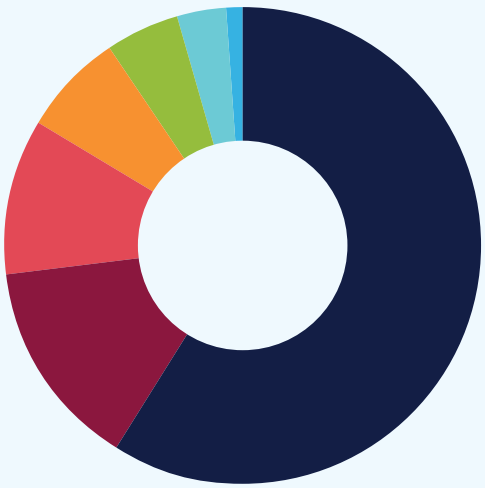
280 Ibid, Article 2.

281 Disciplinary Liability System in Law Enforcement Agencies, EMC, 2017, p. 4, available at: https://goo.gl/mbn3iG

282 E.g. the Regulations of the Ministry of Internal Affairs of Georgia provides for the "hotline" of the General Inspectorate. See: Order of the Minister of Internal Affairs of Georgia M 123 On Approval of the Regulations of the General Inspectorate (Department) of the Ministry of Internal Affairs of Georgia, Article 6(c).

During the reporting period the General Inspectorate has conducted 603 internal inspections, of which in 453 cases the disciplinary measures were applied, the types of which are described on Diagram 3 in details.

STATISTICS OF APPLICATION DISCIPLINARY MEASURES DURING THE REPORTING PERIOD



4	Demotion
16	Dismissal
22	Pulling regular pass
32	Admonition
47	Reprimand
64	Severe reprimand
268	Imposition of up to three extra duties

Pursuant to the Regulations of General Inspectorate an information statement or opinion is drafted about the outcomes of internal inspection, which is approved by the Head of the General Inspectorate. Based on such opinion/statement the Head of the Service makes a decision on the imposition of the disciplinary liability.[283] This means that an opinion on official misconduct is of recommendatory nature and final decision on the application of disciplinary measures is made by the Head of the State Security Service, and in doing so the latter enjoys, in fact, unlimited discretion.
The Law does not provide for any difference between a statement and an opinion issued as a result of the inspection of the General Inspectorate. The practice evidences, that a recommendation on the application of a disciplinary measure as a result of the Inspectorate inspection is made in terms of an opinion, and in the case of existence of a violation - in terms of a statement. It should be mentioned, that if, based on the outcomes of the inspection, the General Inspectorate finds, that there has been no official misconduct, the law does not provide for appeal mechanism.[284]

If, internal inspection, carried out by the General Inspectorate, reveals the elements of a crime, then the situation exceeds the terms of reference of the General Inspectorate and the law in force obligates the latter to immediately refer the existing materials to Chief Prosecutor's Office.[285] The society at large, NGOs and the Public Defender have been claiming the investigation of alleged violations of State Security Service officers by the Prosecutor's Office for years now. They are calling the government to review the existing legislation and create independent investigation mechanism, which will ensure impartial investigation of similar cases.[286] [287]

283 Law of Georgia on State Security, Article 6 (g).

284 The court of law regards an opinion and statement as an interim act, which does not give rise to any legal consequences. In the case of an opinion, an act, issued by the Head of the State Security Service on its bases can be appealed, and in the case of a statement no act is issued. Respectively, it is practically impossible to appeal non-initiation of proceedings. For details see Disciplinary Liability System in Law Enforcement Agencies, EMC, 2017, p. 22-24.

285 Law of Georgia on State Security, Article 50.

286 See Written Communication to the Council of Europe Committee of Ministers from Coalition for an Independent and Transparent Judiciary http://coalition.ge/index.php?article_id=145&clang=0

287 With regard to recommendation of the Public Defender see: "Outcomes of the study of the Public Defender of Georgia,

Recommendations:

- Creation of the efficient mechanism of application to General Inspectorate by citizens;
- To obligate the Head of the State Security Service to initiate disciplinary proceedings against a submission of the General Inspectorate;
- Provision for the possibility of appealing with the court of law in the case of non-confirmation of a misconduct as a result of inspection;
- To provide for the obligation of the General Inspectorate to proactively use performance statistics;
- Creation of legal guarantees for the independence of the General Inspectorate.

disciplinary proceedings against the employees of the Prosecutor's Office of Georgia, Ministry of Internal Affairs, Penitentiary and State Security Service of Georgia on the basis of individual complaints" http://www.ombudsman.ge/uploads/other/4/4923.pdf

CHAPTER 5. TRANSPARENCY OF SECURITY SERVICE SYSTEM

5.1 PUBLICITY OF THE STRUCTURE, FUNCTIONS AND REGULATION OF THE SECURITY SERVICE

According to internationally recognized, the most fundamental standard the security services are to be created on the basis of publicly available laws. According to Practice 4 of the UN Compilation of Good Practices "*All intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be instructed to undertake activities that are prescribed by and in accordance with national law*."

In Georgia the functions of the State Security Service are defined by the Law of Georgia on State Security Service and the Regulations of the Service. The Law defines the fields of activities of the Service in general (protection of constitutional order, protection against unconstitutional change of the regime, protection against terrorism, combating corruption, etc.[288]). This provision is transposed into the Regulations unchanged and it does not provide for further detailed description of the fields of activities of the State Security Service.[289]

The Regulations divide the Service into 13 structural units[290] and defines their main tasks.[291] Of these 13 structural units the Regulations of the following 5 units are classified:

- Information-Analytical Department;
- Counter-intelligence Department;
- State Security Department
- Counterterrorist Centre (Department);
- Special Operations Department.

Consequently, the normative framework of the above Departments is limited to only a small stipulation, contained in one subparagraph of the Regulations of the Service.[292]

Furthermore, the classification of a department Regulations contradicts the law of Georgia on State Secrecy. A dispute within this regard between the EMC and State Security Service is still pending at the Supreme Court of Georgia.[293] In its claim of appeal ECM stated, that classified Regulations do not meet the preconditions, prescribed by the Law of Georgia on State Secrecy for the recognition of information as state secrecy.[294] The Regulations provide for the organizational procedure and principles, rights and obligations and functions of the departments and do not contain any information about intelligence, counterintelligence and operative-investigative activities and covert investigative action plans and specific operations. Tangency on information with intelligence, counterintelligence and operative-investigative activities is not sufficient for the recognition of information as state secrecy. In the case of such wide interpretation of the Law, the Law of Georgia on State Security Service and the Regulations of the Security Service should also be classified as state secrecy. It is necessary to establish, whether or not there is any information from the exhaustive list contained in Paragraph "d.a" of Article 6 of the Law of Georgia on State Secrecy. The Regulations of individual departments cannot contain any information, envisaged by the above Paragraph, the disclosure of which information may jeopardize sovereignty, constitutional order, political and economic interests. Apart

288 For full list see: Law of Georgia on State Security Service, Article 5.

289 Compare: Resolution N385 of the Government of Georgia, dated 30 July, 2015 On Approval of the Regulations of the State Security Service of Georgia, Article 3.

290 Ibid, Article 6.

291 Ibid, Article 7.

292 Ibid, Subparagraphs "e", "g", "h" and "i".

293 See Ruling of the Tbilisi Court of Appeals, dated 16 November, 2017
https://drive.google.com/file/d/1RGTtus3QBcU71Oba4B25jZ9-qRK1aC3J/view

294 See: Law of Georgia on State Security Service, Article 1, Paragraph 1, which is further detailed in Article 6(d.a).

from that, the General Administrative Code of Georgia provides for information, which cannot be classified and this information includes the description of the structure of public institutions, job descriptions of the personnel, also the decision making procedure.[295]

Furthermore, the Law of Georgia on State Secrecy prohibits the classification of information, that may restrict human rights and fundamental freedoms, as state secrecy.[296] It should be mentioned, that certain functions, performed by the department with secret Regulations, are closely linked with human rights and fundamental freedoms and their restriction. Specifically, according to the Regulations of the State Security Service the main tasks of the Counterintelligence Department are: conduct of operative-investigative operations in accordance with the procedure, prescribed by law; application of coercive measures, envisaged by the Code of Criminal Procedure, with regard to cases falling under its jurisdiction and investigation of criminal cases; also the implementation of preventive measures for crime exposition and suppression.[297] Similar coercive and preventive tasks are delegated to State Security Department and Counterterrorist Centre (Department).[298] It is apparent, that the activities of these Departments may restrict human rights and basic freedoms and the Regulations of the Department cannot be regarded as "regulating internal activities".[299]

The right of freedom of information is guaranteed by Paragraph 1 of Article 41 of the Constitution of Georgia and restriction of the access to requested information constitutes an intervention into this right. However, this right is not an absolute one and it can be restricted in full compliance with relevant formal and material requirements. Formal compliance requires for any restriction on the access to information to be envisaged by law. Classification of a Department Regulations is not compatible with the Law of Georgia on State Secrecy, it is not classified according to law and thus it violates the Constitution as well.

The practice of secret sublegal acts (orders of the Minister, etc.) is also based on international experience. Such regulations often contain the description of performance procedures and operational methods of security services, the disclosure of which may jeopardize the flow of operations of the Security Service.[300] However, inclusion of such stipulation of secret nature in a department Regulation does not provide for the classification of the whole Regulations, but rather demonstrates, that it is included in a wrong act, thus endangering the transparency of the activities of the whole Department.

As regards secret acts, according to UN guidelines, the use of subsidiary regulations is strictly limited. Regulations that are not made public do not serve as the basis for any activities that restrict human rights.[301] E.g. the scope of surveillance, conducted by these services should be regulated by law and not secret directives.

5.2 REQUEST OF PUBLIC INFORMATION FROM SECURITY SERVICE AND THE RIGHT TO ACCESS OWN PERSONAL DATA

5.2.1 ACCESSIBILITY OF PUBLIC INFORMATION IN STATE SECURITY SERVICE

The classified nature of State Security Service activities renders impossible to apply the general standard of transparency of state authorities thereto. However, the scope of secret activities of the security system cannot justify its total seclusion in the light of freedom of information. Absolute non-transparency of the system provides for its inefficient performance, decreases public confidence towards the institution and makes the efficient oversight impossible.

The Georgian law provides for rather high standard of accessibility of public information. Specifically, public

295 General Administrative Code of Georgia, Article 42 (c).

296 Paragraph 1 of Article 7.

297 Resolution N385 of the Government of Georgia, dated 30 July, 2015, On Approval of the Regulations of the State Security Service, Article 7(g).

298 Ibid, Subparagraphs "h" and "j".

299 Article 19(i) of The List of Information Classified as State Secrecy (Appendix M12) of the Government of Georgia Resolution N507, dated 24 September, 2015 on Approval of Normative Acts Related to Putting the Law of Georgia on State Secrecy in Force, allows for the classification of internal normative acts of the State Security Service if they regulate their *internal performance* in the respective fields.

300 Aidan Wills, Understanding Intelligence Oversight,(DCAF.2010) p.14.

301 UN Compilation of Good Practices, Practice 4.

information is open except for cases, envisaged by law and information attributed to personal data, state or commercial secrecy in accordance with the established procedure.[302]

The Law on State Secrecy prescribes whether which information can be classified as secret in intelligence, state security and law enforcement fields.[303]

The Global Principles on National Security and the Right to Information provided for the overwhelming standard for such restrictions. According Principle 3: "No restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: "

1. The restriction:
    - is prescribed by law
    - is necessary in a democratic society
    - to protect a legitimate national security interest.
2. The law provides for adequate safeguards against abuse, including prompt, full, accessible, and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts."

This standard imposes the burden of proof of the necessity of restriction on the government, highlights the legitimization of the national security interests and considers it necessary to introduce the efficient mechanism of external and judicial oversight.

Although in most cases the restriction of the access to information is based on the interests of protection of "national security", there is no mandatory and exhaustive list at international level, whether which information should be classified. Despite the foregoing, based on expert opinion and the best international practice, the Global Principles on National Security and the Right to Information provided for the list of such information, the access to which may be restricted lawfully. Specifically[304]:

- Information about on-going defense plans, operations, and capabilities for the length of time that the information is of operational utility;
- Information about the production, capabilities, or use of weapons systems and other military systems, including communications systems;
- Information about specific measures to safeguard the territory of the state, critical infrastructure, or critical national institutions (institutions essentielles) against threats or use of force or sabotage, the effectiveness of which depend upon secrecy;
- Information pertaining to, or derived from, the operations, sources, and methods of intelligence services, insofar as they concern national security matters;
- Information concerning national security matters that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality; and other diplomatic communications insofar as they concern national security matter.

Although Georgian legislation is in line with the aforementioned basic international principles, there still are problems with regard to implementation and interpretation of the law. Because of incorrect interpretation of Law even such information is classified as secret, as the Regulations of the State Security Service, which, as a general rule, should contain information only about the structure and functions.

The following basic problems were identified as a result of requesting information from the State Security Service within the framework of the research,:

- The State Security Service does not issue information within timelines specified by Law (immediately or in exceptional cases - within a period of 10 days);
- The State Security Service classifies information without any grounds and, relevantly, would not issue it;

302 General Administrative Code of Georgia, Article 28, Paragraph 1.

303 Law of Georgia on State Secrecy, Article 6.

304 Tshwane Principles, Part II, Principle 9.

- In the case of non-issuance of information, the State Security Service does not provide reasons of non-issuance of the information.

For example, the State Security Service has not provided us with the following statistic data:

- Number of motions filed with the court and satisfied with regard to conducting electronic surveillance;
- Number of motions filed with the court and satisfied with regard to conducting covert investigative operations;
- Number of employees of the State Security Service, according to structural subdivisions.

The State Security Service provided us with the following data: about salaries, official allowances and bonuses issued to the employees of the State Security Service according to years; sublegal normative acts, regulating personnel related issues (recruitment, dismissal, promotion, evaluation of personnel, issuance of official allowances, etc.) in the State Security Service; whether or not the Regulations of some Department of the State Security Service was classified or declassified during the period between the first of August, 2015 and inclusive 31st of December, 2017 (number); number of dismissed and recruited personnel; number of complaints reviewed by the General Inspectorate and number and types of imposed penalties, also the number of initiated investigations.

It should be stressed that the State Security Service does not give reasons of non-issuance of information, what is also contrary to law. According to Article 41 of the General Administrative Code of Georgia, in the case of refusal to issue public information a public authority is required to give written explanations to the person concerned about his rights and appeal procedure, also specify the structural subdivision or public institution, which was consulted when making a decision on refusal to issue the information.

Worth mentioning is the Decision of the Court of Appeals on the action of Human Rights Education and Monitoring Center (EMC), delivered on 16 November, 2017. The Decision finds rather low standard of issuance of information by the State Security Service.

The EMC appealed non-issuance of the following information by the State Security Service:

1. Number of employees of the State Security Service according to structural subdivisions of the Service;
2. Monthly rates of salaries attached to the position and rank of the Service employees;
3. The list of structural subdivisions, that are entitled to conduct investigation under the Code of Criminal Procedure of Georgia;
4. Statistic data about the investigations launched by the State Security Service according to the Code of Criminal Procedure (with reference to relevant articles of the Criminal Code and subdivisions of the Service, which conduct ongoing investigation) from the date of its creation.
5. Information about the legality of setting up of the ad hoc commission, which is to ensure the inventory taking of the assets/documentation (in the case of setting up the commission - the composition thereof).

The City Court and the Court of Appeals have not met the claim and respectively, non-issuance of this data by the State Security Service was found legal. The case is currently reviewed by the Supreme Court of Georgia. We are of the opinion, that the court decision is not duly reasoned and is not compatible with Global Principles on National Security and the Right to Information, particularly in its part, which concerns statistic data, publicity of Regulations and existence of investigative function of the subdivisions.

5.2.2 STANDARD OF ACCESS TO OWN PERSONAL DATA

One of the key criteria of evaluation of the transparency of public institutions is the right to access personal data held by public sector.

Right of an individual to receive information about data held by a state authority about him/her is the right guaranteed by the Constitution of Georgia. Every citizen of Georgia is entitled to become acquainted, in accordance with a procedure prescribed by law, with the information about him/her stored in state institutions

as well as official documents existing there unless they contain state, professional or commercial secret.[305]

Despite the rather high standard of protection of this right, guarantees by the Constitution, the problem with the accessibility of personal data in security sector is conditioned by following reasons:

1. The practical interpretation of security purposes is rather wide and does not contain clear criteria of restriction;
2. There is no oversight of the protection of personal data in State Security Service as Personal Data Protection Inspector has no access to classified information held by the State Security Service. And there is no other institution to oversee the protection of person data.

The Law on Personal Data Protection provides for restriction, which renders it impossible for Personal Data Protection Inspector to exercise comprehensive oversight of State Security Service. Specifically, according to the Law on Personal Data Protection, the Law does not apply to procession of information for state security (inter alia, economic security), defense, intelligence and counterintelligence purposes.[306] Therefore, Personal Data Protection Inspector is not in the position to review a case on access to personal data held by State Security Service either on his own initiative or on the basis of the complaints of the citizens.

In international law the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[307] is the first binding legal instrument, which sets data collection and procession standards and which explicitly acknowledges the rights of data subject (with regard to whom the data are collected).[308]

The provisions of this legally binding Convention provides for explicit obligations of security services to address requests concerning personal data, communicate data to data subject, ensure the rectification or erasure of personal data in the case of their unauthorized collection/ procession. However, Article 9 of the Convention allows for the security services to derogate from such obligations in the interests of "protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences" and "protecting the data subject or the rights and freedoms of others."

The international standards are acknowledged not only by the Council of Europe Convention, but also by the instruments of the international law of recommendatory nature, like US Guidelines for the Regulation of Computerized Personal Data Files (Principle 4),[309] Global Principles on National Security and the Right to Information (III Part), also the UN Compilation of Good Practices (Practice 26). According to these European and international standards, most of the democratic countries adopted relevant national laws and provided for the mechanisms for the protection and exercise of the right to access own personal data. There are three main approaches with regard to this issue:

Direct access of data subject to data: Many States have laws giving individuals the right to have access to their personal data held by intelligence services. However, these laws provide for certain restrictions as well, allowing security services not to provide information to the individual for reasons such as safeguarding ongoing investigations and protecting sources and methods of the security services.[310] In this regard the important standard is for such exceptional cases to be explicitly provided for by law and the law should provide for the right of data subject to appeal this decision with the court of law.[311]

---

305 The Constitution of Georgia, Article 41.

306 For details see Chapter 3.5.1. of the survey.

307 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

308 According to Article 8"Any person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention; to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs 'b' and 'c' of this article is not complied with."

309 General Assembly Resolution 45/95 (1990), available from : http://www.refworld.org/pdfid/3ddcafaac.pdf

310 UN Compilation, Para. 40.

311 Laurie Nathan, 'Intelligence Transparency, Secrecy and Oversight in a Democracy', p.55 in Born and Wills (ed.) Overseeing Intelligence Services: A Toolkit (DCAF: 2012)

Indirect access through an expert oversight body or Personal Data Protection Agency (DPA): To balance restrictions on data subject's access to data some states grant the right to access these data in their name and on their behalf to data protection or/and expert oversight authorities. In this light an example of the best practice is the situation, when these authorities are entitled to check, whether or not the restriction of data subject's access was well-reasoned, to review these data to verify, whether or they were collected/ obtained legally and decide on the destruction of the data in the case of detection of any breach of law.[312] This approach is adopted in 12 EU Member States, including Austria, Belgium, Bulgaria, Cyprus, Finland, France, Hungary, Ireland, Italy, Luxembourg, Portugal and Sweden.[313]

Provision of a notice to data subject by security service: The latest, however not yet wide-spread approach is obligating security services to inform data subject after the accomplishment of secret surveillance operations against the former irrespective of the request of the data subject concerned or/and expert oversight authority.

The above approaches are not mutually excluding and a country may apply them jointly.

312 EU FRA, Surveillance by Intelligence Services ,Vol. 2, (2017), p.110, Also see Hans Born and Ian Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies, (DCAF: 2005)

313 EU FRA, Surveillance by Intelligence Services Vol. 2, (2017), p.126.

5.3 THE BEST PRACTICE OF SELECTED COUNTRIES

Transparency of state security services.

Country	Does the State Security Service conduct its work on the basis of a publically available law?	How is access to information regulated?	In what cases can information be confidential?	What forms of accountability does the State Security Service use?
Germany	Both the BfV and the BND operate based on publicly available laws	At the federal level, the right to access to information is regulated by the Freedom of Information Act	Information can be confidential, if it damages: • International relations,, • Military and other security-critical interests of the Federal Armed Forces, • Internal or external security interests, • Monitoring or supervisory tasks of the financial, competition and regulatory authorities, • Matters of external financial control • Measures to prevent illicit foreign trade • the course of current judicial proceedings	BfV annual report
Canada	The Canadian Security Intelligence Service (CSIS) operates based on a publicly available law	Access to information is regulated by Access to Information Act. The Act stipulates the exemptions from the Government's duty to disclose information	The Government has the right to refuse disclosing information if it poses a risk the security of the state, ongoing operations.	CSIS's annual reports are exemplary, as it provides comprehensive information on the service. It publishes the number of employees, as well as statistics on diversity. Moreover, the report has data on general breakdown of the budget into operational costs and salaries.

Croatia	The Croatian security service (SOA) operates based on a publicly available law, but there are exemptions from the Government's duty to disclose information.	Access to information is regulated by the Law on the Right to Access to Information. Article 15 of the law has a long list of conditions which would restrict public access to information, one of which is 'if the information is classified by public authorities'	The director of the SOA is entitled to classify information whose disclosure would damage national security or functioning of state authorities	SOA publishes annual reports, which include an overview of main security challenges, security vetting activities of SOA, information on international cooperation and very basic information on the budget.
Belgium	Belgian security services are constituted through and operate based on publicly available laws	Access to general information held by the services, as well as one's own data is regulated by the Act on the Transparency of Administration.	The security service is not obliged to disclose the data, if it deems safeguarding the interests of public order, public security, national defence and the safety of the population are more important than principle of transparency	Annual reports are prepared by the Belgian security service

5.4 SUMMARY/RECOMMENDATIONS

Maintenance of balance between the classification and transparency of the activities of the Secret Service is of paramount importance both for efficient performance of the Service, on one hand, and efficient oversight of the Security service, on the other.

Overwhelming classification of Service activities provokes further deepening of distrust in the Service, on the one hand, while on the other - the oversight authorities will never be able to duly oversee the lawfulness and efficiency of the Security Service policy and performance without sufficient information.

The law does not provide even for minimal standards of Service accountability and transparency. The wording of the Law of State Secrecy with regard to classification of a normative act is quite ambiguous. Almost every statistic data are regarded as confidential information. The Parliamentary Report of the Head of the Service is very general and does not provide the society at large with comprehensive information about the situation in the country in the light of security. Furthermore, the Report does not say anything about statistics that is unduly regarded as state secrecy.

Based on best international practice is will be reasonable to implement the following changes:

- To make public classified Regulations of the State Security Service Departments;
- An annual report submitted to the Parliament by State Security Service should contain all statistic data about accomplished operations; also the information about net amounts allocated from the budget for salaries and for the coverage of the costs and expenses of the operations. The report should contain information about received complaints and their review by oversight authorities. The classified part of the report should be reviewed by a special oversight body of the Parliament.
- The questions related to the issuance of public information should be addressed in accordance with Global Principles on National Security and the Right;
- The Service is to fulfill the obligation, envisaged by General Administrative Code with regard to publication of full reports on the issuance of public information (the so-call "10th of December Reports");
- The law should explicitly provide for the standards of access of an individual to own personal data, when this information is held by the State Security Service. The information can also be accessed through an oversight authority. The grounds for a restriction should be exhaustively and explicitly provided for by the law.