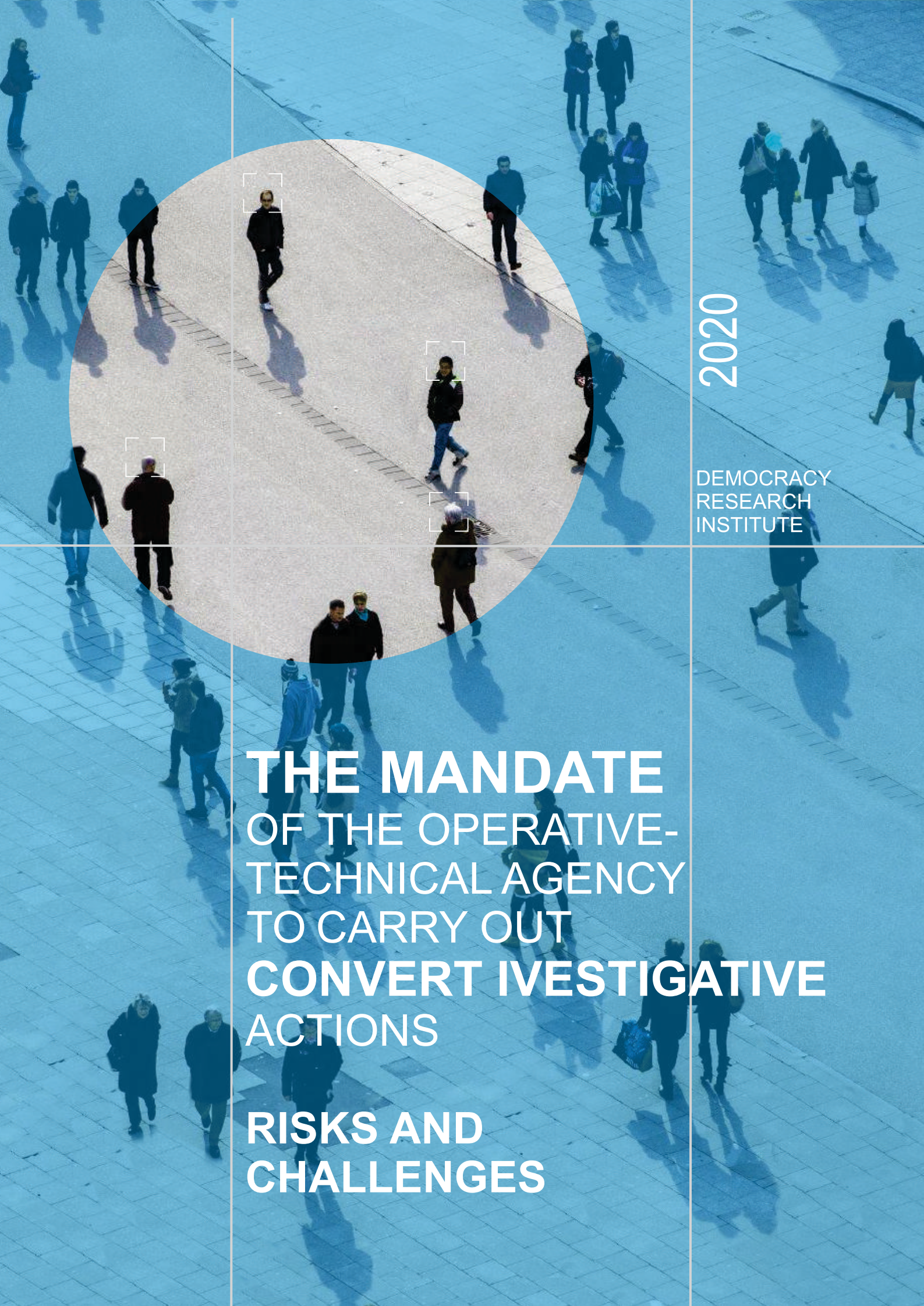

2020

DEMOCRACY
RESEARCH
INSTITUTE

THE MANDATE
OF THE OPERATIVE-TECHNICAL AGENCY TO CARRY OUT **CONVERT IVESTIGATIVE** ACTIONS

RISKS AND CHALLENGES

Contributors to the Report: Giorgi Tsikarishvili, Tatia Koniashvili and Tamar Khidasheli

Responsible for the Publication: Ucha Nanuashvili

English text editor: Vikram Kona

The report is developed by the Democracy Research Institute (DRI), within the project Supporting Security Reform System in Georgia. The financial support of the project is provided by the National Endowment for Democracy (NED). The views and opinions expressed in the publication are those of the project team and do not necessarily reflect the official position of the donor organisation.

TABLE OF CONTENTS

INTRODUCTION

Special investigative actions (covert investigative/operative and investigative actions) imply gathering evidence through various devices and means, without giving a prior notification to individuals concerned. These actions are carried out by specially authorised state agencies. The means employed during covert investigative actions usually limit the right to respect for private life. This problem has become even more relevant due to the development of increasingly sophisticated surveillance technologies. There are two conflicting fundamental interests in the process of covert investigative actions, viz., the public interest of identifying an offender and thus protecting others' rights on the one hand and, on the other hand, the right to respect for private life. For enforcing the judgment of the Constitutional Court of Georgia adopted on 14 April 2016,[1] since 22 March 2017, covert investigative actions have been carried out in Georgia by the LEPL Operative-Technical Agency of Georgia.[2] This agency is subordinate to the State Security Service. However, those problems highlighted by the Constitutional Court in the above judgment have not been substantially eliminated.

This research aims at critically assessing the measures taken for enforcing the Constitutional Court's judgment by the Parliament of Georgia and highlighting the problems and shortcomings regarding the powers of the Operative-Technical Agency and the mechanisms of oversight over the agency. The research endeavours at elaborating concrete recommendations based on international practice and experience and contributing to their implementation.

The first chapter of the research deals with the evolution of the legislative regulation of covert investigative actions. It focuses on the incidents of illegal wiretapping, the importance of the 2015 reform of the State Security Service, the 14 April 2016 judgment of the Constitutional Court and its implementation. The second chapter discusses the formal and legal grounds for covert investigative actions. The third chapter constitutes the main body of the research. It describes the powers of the Operative-Technical Agency and discusses the problems potentially endangering human rights and freedoms. The fourth chapter assesses the compatibility of the mandate of the Operative-Technical Agency with international standards. The fifth chapter covers other procedural issues related to covert investigative actions; it studies and analyses existing legislative problems. The next chapter deals with the importance of judicial sanctioning of covert investigative actions and highlights existing problems in the light of relevant international practice. This section of the report also discusses discontinuation of covert investigative actions, the procedure of retaining and destruction of information gathered as a result of covert investigative actions as well as legal safeguards for the object of surveillance determined by Georgian legislation. The research discusses the oversight mechanism of the State Inspector's Service over covert investigative actions and critically assesses vesting this agency with investigative powers. The concluding part of the research gives recommendations elaborated by the Democracy Research Institute (DRI).

[1] See judgment №1/1/625,640 of the first section of the Constitutional Court of Georgia, adopted on 14 April 2016.
[2] The Law of Georgia on the LEPL Operative-Technical Agency, Article 7.

RESEARCH METHODOLOGY

The present research studies the activities of the Operative-Technical Agency from 22 March 2017 to date, notably, whether the agency without the relevant legal grounds can directly access commun-ication between wide groups of citizens.

Following the judgment adopted by the Constitutional Court of Georgia on 14 April 2016, the DRI studied the changes made to the legislation governing covert investigative actions, especially the powers of the Operative-Technical Agency, and the oversight mechanisms concerning its activities.

This research is also based on the analysis of data posted on the public agencies' websites. Furthermore, the report has cited documents and viewpoints of international organisations regarding the reform of the security system.

Objects of the research: the State Security Service, the Operative-Technical Agency under the State Security Service, the Ministry of Internal Affairs, the Prosecutor's Office of Georgia, the State Inspector's Service and the judiciary.

Processing and analysing data: at the initial stage of the research, we made a list of the normative acts to be studied and processed the data obtained through requesting public information.

Methodology: situation analysis method was employed in the research process. Notably, in terms of reforming the State Security Service, we studied the experience of those countries that, keeping the local context in view, can be considered to be the best examples. In particular, we selected the following six countries:

- **Latvia and Lithuania** were selected due to their geopolitical location, post-Soviet experience and successful reforms in the security sector;
- **Estonia** is distinguished due to the results achieved in the field of security, particularly in the cybersecurity sector, as well as its exemplary cooperation with NATO and EU security agencies;
- **Ukraine** and Georgia are faced with similar challenges in terms of security. With the support of the international community, numerous reforms, based on international standards, have been carried out for legislative and structural enhancement of the Ukrainian security sector. The Ukrainian experience is significant to Georgia;
- **Norway** was selected due to exemplary distribution of functions among law-enforcement, intelligence and security services as well as the effective steps taken towards the fight against extremism and radicalisation; and
- **Canada**, despite its expressly distinct legal framework, is often referred to in international organisations' researches as an example of best practice.

Descriptive statistics analysis – qualitative description of the information requested from agencies, i.e., maintaining descriptive statistics.

Desk Research implies gathering, analysing and using public data in a research process that has been published by administrative agencies proactively.

1. RELEVANCE OF THE PROBLEM OF COVERT INVESTIGATIVE ACTIONS AND LEGISLATIVE REGULATION IN GEORGIA

The Constitution of Georgia declares and protects the rights to respect for private and family life, personal space and communication.[3] There are risks of interference with these rights when conducting investigative actions.

Before 2014, the procedure of employing covert methods by law-enforcement bodies was regulated by the Law of Georgia on Operative and Investigative Activities.[4] Under this version of the law, the use of covert methods, as an operative and investigative action used to take place under a judge's order after the institution of a criminal case.[5] Such wording of the law gave rise to the possibility of using covert methods before the institution of a criminal case. An operative and investigative action without a judge's order implies preventive actions when there is no investigation instituted and yet a relevant body can resort to covert methods. The amendments made in 2014 added a new chapter, Chapter XVI[1], to the Criminal Procedure Code of Georgia on Covert Investigative Actions[6] extending prosecutorial and judicial review to such actions.[7]

Under the legislation in force, covert investigative actions are conducted when an investigation has been initiated and/or criminal prosecution is conducted into an intentional and serious and/or particularly serious crime or a crime under relevant articles of the Criminal Code of Georgia.[8] In accordance with the changes made in 2019, covert investigative actions are applied with regard to crimes under Chapter XXXIX[9], i.e., to all official misconducts. Accordingly, now it is possible to conduct covert investigative actions concerning crimes committed by negligence.[10] This further increases the risk of serious interference with human rights.

1.1. INCIDENTS OF ILLEGAL WIRETAPPING IN GEORGIA AND RESPECTIVE LEGISLATIVE CHANGES

In September 2012, video recordings depicting the torture of prisoners in penitentiary establishments were disseminated, causing a backlash in the public. Later, it was revealed that there were other covert recordings with the Ministry of Internal Affairs. Some of them were destroyed by the commission set up under a governmental resolution and some of them were submitted to the Chief Prosecutor for investigation.[11]

On 1 August 2014, Article 143[10] was added to the Criminal Procedure Code.[12] This provision imposed a duty on the Supreme Court of Georgia to publish at the end of each year statistical data

[3] The Constitution of Georgia, Article 15.
[4] The Law of Georgia on Operative and Investigative Activities, as of 1999-2014.
[5] *Ibid.,* Article 7.3.
[6] The Criminal Procedure Code, Chapter XVI[1], as of 01.08.2014.
[7] The Criminal Procedure Code, Article 143[3].
[8] *Ibid.,* para. 2.a).
[9] *Ibid.*
[10] For instance, a crime under Article 342 of the Criminal Code (neglect of official duty) can only be committed by negligence.
[11] See final report by the temporary commission on illegal wiretapping and covert recordings, 31.01.2014, accessible http://gov.ge/index.php?lang_id=geo&sec_id=397.
[12] The Law of Georgia no. 2634 of 1 August 2014, 18.08.2014.

pertaining to covert investigative actions, among them, the number of motions for covert investigative actions filed with courts.

The disclosure of illegal video recordings made it necessary to amend the Law of Georgia on Electronic Communications. This also implied the restriction of law-enforcement agencies' direct access to telecommunication data. The version of the draft law that maintained the power of conducting covert surveillance for the Ministry of Internal Affairs[13] caused a backlash from civil society. Though the president vetoed the draft law, the parliament overruled the veto and the Ministry of Internal Affairs retained the duty of retaining gathered information for another two years.[14] The Criminal Procedure Code was amended as well.[15] Based on this, the electronic system of two-stage covert investigative actions was introduced.[16]

Despite the above-mentioned, the problem of illegal wiretapping continued in the following years as well.[17] Leaders of opposition political parties and journalists were the main target of unauthorised wiretapping.

1.2. THE REFORM OF THE STATE SECURITY SERVICE

As a result of the reform carried out in August 2015, the State Security Service was separated from the Ministry of Internal Affairs and it was set up as an independent agency. According to a pre-election promise of Georgian Dream, the State Security Service's powers were to be limited to gathering intelligence, its analysis and systematisation. According to the pre-election programme, the service was supposed to be stripped of its criminal prosecution powers.[18] Despite this promise, the service was vested with both analytical and investigative powers,[19] including the powers to have direct access to active lines of electronic communication (to conduct covert investigative actions).[20]

1.3. JUDGMENT NO. 1/1/625 OF THE CONSTITUTIONAL COURT OF 14 APRIL 2016 AND ITS EXECUTION

In 2015, a constitutional complaint was lodged with the Constitutional Court of Georgia in which applicants challenged the constitutionality of certain provisions of the Code of Criminal Procedure of Georgia and the Law of Georgia on Electronic Communications that gave the State Security Service a technical possibility to obtain information from actual lines of communications in real-

[13] The Law of Georgia on Electronic Communications, Article 8^3, Law of Georgia no. 2871 of 30 November 2014, 30.11.2014; see the Criminal Procedure Code, Article 3.32, the version in force before 01.08.2015.
[14] The Law of Georgia on Electronic Communications, Article 8.3, 01.08.2014.
[15] The Law of Georgia no. 2870 of 30 November 2014, 30.11.2014.
[16] The set of technical and software solutions that excludes the possibility of independently carrying out an order on the activation of an object through the monitoring system of a law-enforcement body without the electronic permission of the Personal Data Protection Inspector.
[17] More details about incidents of illegal wiretapping, see: http://liberali.ge/news/view/31277/TI-gakhmaurebuli-saqmeebis-gamodziebis-shesakheb-informatsia-dakhurulia.
[18] Pre-election programme of Georgian Dream, 2012, p. 18, available at: http://www.ivote.ge/images/doc/pdfs/ocnebis%20saarchevno%20programa.pdf.
[19] The Law of Georgia on the State Security Service of Georgia, Article 11.
[20] The Law of Georgia on Electronic Communications, Article 8^3, Law of Georgia no. 3929 of 8 July 2015, 15.07.2015; the Criminal Procedure Code, Article 3.32, the version in force before 22.03.2017.

time without adequate oversight mechanisms.[21] The applicants also alleged that under those circumstances, where the State Security Service enjoyed a virtually uncontrolled possibility to access communication means, there was a serious risk of mass surveillance of the public [22] which is against the right of free development of an individual and right to respect for private life safeguarded by the Constitution.

The Constitutional Court declared the impugned provisions unconstitutional and observed that the existing regulations failed to ensure that wiretapping of telephone conversations and retrieval and recording of information were conducted only based on a court order or in the case of urgency (with a court order issued *ex post facto*). Therefore, the impugned provisions contradicted Article 20 of the Constitution.[23] Furthermore, under the conditions of the lack of solid, sufficient and effective safeguards for confidentiality and inviolability, the Court found that because the State Security Service possessed identification data there was an unjustified and intrusive interference with the right to free development of an individual.[24]

The Constitutional Court's judgment was followed by legislative amendments, in particular, the so-called "two-key system" was abolished; the Personal Data Protection Inspector was given the authority to suspend a covert investigative action.[25] Paragraph 4 was added to Article 35 of the Law of Georgia on Personal Data Protection which determined the scope of the Inspector's powers in terms of inspecting the agency,[26] which, however, had been already in place in accordance with the Personal Data Protection Inspector's order.[27]

The Operative-Technical Department was replaced by the Operative-Technical Agency under the State Security Service, which was vested with the power of conducting covert investigative actions under the relevant law.[28] As regards the retention of electronic communication identification data, it was determined that the agency had the power to retain this data for up to 12 months.[29] This way, the Constitutional Court's judgment was ignored as the service maintained the impugned power. In 2016, the Public Defender of Georgia and 326 individuals reapplied to the Constitutional Court and requested the declaration of a number of provisions as unconstitutional that had been added as a result of legislative amendments to the Law of Georgia on Electronic Communications and the Criminal Procedure Code of Georgia. The Court, despite dissenting opinions of three judges of the plenum, did not find that the impugned provisions overcame the Constitutional Court's judgment of 14 April 2016 and ruled in favour of the examination of the merits of the constitutional complaint.[30]

In 2019, the Office of the Personal Data Protection Inspector was abolished and the State Inspector's Service was set up. This office was vested with the powers to inspect the legality of both investigative actions and personal data processing.[31]

---

[21] Judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016, para. 36.
[22] *Ibid.,* para. 86.
[23] *Ibid.,* para. 83.
[24] *Ibid.,* para. 115.
[25] See the Criminal Procedure Code, Article 143[6].5, 22/03/2017.
[26] The version of the law as of 22/03/2017.
[27] Order no. 1 of the Personal Data Protection Inspector of 4 March 2016.
[28] The Law of Georgia on the LEPL Operative-Technical Agency, Article 8.
[29] *Ibid*, Article 15.1 and Article 15.2.
[30] The Public Defender of Georgia, Citizens of Georgia – Avtandil Baramidze, Givi Mitaishvili, Nugzar Solomonidze and Others (in total, 326 constitutional complaints) v. the Parliament of Georgia, the decision on admissibility of 29 December 2017.
[31] The Law of Georgia on the State Inspector's Service, Article 2.

2. FORMAL AND LEGAL GROUNDS FOR COVERT INVESTIGATIVE ACTIONS

Security services have great potential for interfering with fundamental human rights, notably, the right for respect for private life. This problem is particularly relevant when security services resort to the means of targeted surveillance such as wiretapping telephone conversations or installing listening devices at a person's residence.

In Georgia, under the legislation in force, the LEPL Operative-Technical Agency[32] under the State Security Service conducts covert investigative actions as per the Criminal Procedure Code.[33] Given the fact that the State Security Service is vested with the investigative power[34] and is interested in the prompt investigation of a concrete case, the Operative-Technical Agency cannot be deemed to be an independent body thus giving rise to a real risk of disproportionate interference with human rights.

2.1. FORMAL GROUNDS FOR COVERT INVESTIGATIVE ACTIONS

Covert investigative actions are conducted when an investigation has been initiated and/or criminal prosecution is conducted into an intentional and serious and/or particularly serious crime or a crime under relevant articles of the Criminal Code of Georgia.[35]

Despite the objection from civil society,[36] with the government's initiative,[37] since 2019, it has been possible to conduct covert investigative actions concerning all official misconducts. Based on these legislative changes, it is allowed to interfere in personal space even when a person allegedly committed a crime by negligence.[38] At the same time, the Criminal Code of Georgia highlights that intent is a *conditio sine qua non*.[39] Therefore, this regulation contradicts the Criminal Procedure Code. A judge, when examining a motion on a covert investigative action, must be guided by these grounds. It is impossible to discuss a covert investigative action as a means of last resort in those circumstances where it can be used regarding a wide range of crimes.

The scope of application of the crimes regarding which covert investigative actions can be used and the range of the use of these actions are relevant in terms of the assessment of the European Court of Human Rights whether the legislation governing interference with the rights safeguarded by Article 8 of the European Convention on Human Rights (the right to respect for private and family life, home and correspondence) met the standards of the quality of the law required by Article 8.2 of the Convention, as interpreted by the Court. Notably, in the case of *Uzun v. Germany,* the European Court of Human Rights observed that because surveillance could only be ordered against

[32] The Law of Georgia on the LEPL Operative-Technical Agency, Article 3 (1).
[33] The Criminal Procedure Code, Article 3.32.
[34] The Law of Georgia on the State Security Service of Georgia, Article 11.
[35] The Criminal Procedure Code, Article 143[3].2.a).
[36] See https://www.transparency.ge/ge/post/paruli-sagamoziebo-mokmedebebis-qvela-samoxeleo-danashaulze-gavrceleba-daushvebelia.
[37] See the Government's initiative on amending the Criminal Procedure Code of Georgia, (07-2/265; 25.10.2018).
[38] For instance, the Criminal Code of Georgia, Article 342 – neglect of official duty.
[39] The Criminal Procedure Code, Article 143[3].2.a).

a person suspected of a criminal offence of considerable gravity or, in very limited circumstances, domestic law thus set quite strict standards for authorising the surveillance measure at issue.[40] This was one of the factors due to which the Court held that the interference with the applicant's right to respect for his private life was "in accordance with the law" within the meaning of Article 8.2.[41]

This circumstance is also relevant in terms of the European Court's assessment whether the interference was "necessary in a democratic society". When assessing the conflict between the applicant's private life and the legitimate aim of the investigation of crimes, the European Court of Human Rights took into consideration the fact that the investigation for which the surveillance had been put in place concerned very serious crimes, namely several attempted murders of politicians and civil servants by bomb attacks.[42] This circumstance was an important factor for the European Court to find that the interference with the applicant's right to respect for private life was proportionate to the legitimate aims pursued and thus "necessary in a democratic society". There had accordingly been no violation of Article 8 of the Convention.

Unfortunately, the existing Georgian legislation does not follow the above approach of the European Court of Human Rights and contradicts it.

In 2019, the court examined 1,037 motions about wiretapping and covert recordings of telephone communications filed by the prosecutor's office.[43] Out of these, 104 motions concerned official misconducts. 100 motions out of such motions were upheld fully; one motion was upheld partially and three motions were rejected.[44] It is noteworthy that all four motions filed with regard to acts categorised under Article 342 of the Criminal Code (neglect of official duty which can be committed only by negligence) were upheld.

The mandate of the State Security Service applies to some official misconducts (among others, crimes under Article 342 of the Criminal Code).[45] Based on international standards, it is recommended to limit state security services' powers to protecting the national interests of the state. Therefore, it is doubtful how a crime committed by negligence, a less serious crime, can endanger state security. The aforementioned, coupled with the absence of solid mechanisms of oversight, increases the risk of abuse of powers by the agency and breach of human rights.

2.2. LEGAL GROUNDS FOR COVERT INVESTIGATIVE ACTIONS

The right to respect for private and family life, personal space and communication, guaranteed by the Constitution of Georgia, "may be restricted only in accordance with law for ensuring national security or public safety, or for protecting the rights of others, insofar as is necessary in a democratic

[40] *Uzun v. Germany*, application no. 35623/05, judgment of the European Court of Human Rights of 2 September 2010, para. 70.
[41] *Ibid.,* para. 74.
[42] *Ibid.,* para. 80.
[43] See the website of the Supreme Court of Georgia, http://www.supremecourt.ge/statistics/2019/.
[44] Comment: this information mainly contains seven months' data. Before 29.05.2019, covert investigative actions applied only to official misconducts under Articles 340 and 341 of the Criminal Code of Georgia. Only one motion has been submitted with regard to a crime penalised under one of these provisions, notably Article 341.
[45] Order no. 3 of the Prosecutor General of Georgia of 23 August 2019 on Determining Investigative Jurisdiction and Territorial Investigative Jurisdiction of Criminal Cases, para.4.c).

society, based on a court decision or without a court decision in the case of urgency provided for by law."[46] Covert investigative actions constitute such means of interfering with these rights that must be "necessary to achieve a legitimate goal in a democratic society, in particular, to ensure national or public security, to prevent riots or crime, to protect the country's economic interests and the rights and freedoms of other persons;" they must be adequate and proportional means of last resort.[47] If a measure interfering with a human right is carried out covertly, the risk of arbitrary action is particularly high and the degree of intrusion intensifies. The authorising body (the court) has to assess the circumstances correctly and allow such restrictions only in those cases where investigative interests outweigh the interest of respecting the right to privacy. The court making the decisions in such cases must strictly observe the relevant statutory requirements.

[46] The Constitution of Georgia, Article 15.

[47] The Criminal Procedure Code, Article 143[2].

3. THE OPERATIVE-TECHNICAL AGENCY AS A BODY CONDUCTING COVERT INVESTIGATIVE ACTIONS AND THE SAFEGUARDS FOR ITS INDEPENDENCE

Creating the LEPL Operative-Technical Agency was aimed at executing the Constitutional Court's judgment that declared regulations governing covert investigative actions as unconstitutional. According to the explanatory memorandum, the agency enjoys independence safeguards[48] and within its competence carries out its statutory tasks independently and within its statutory powers.[49] Despite this, the analysis of the legislation in force and the existing practice demonstrate that the Constitutional Court's judgment has not been executed.

The agency is a legal entity of public law under the State Security Service.[50] Therefore, it is subordinate to the State Security Service, which is vested with investigative powers.[51]

An order of the Prosecutor General of Georgia determines the jurisdiction of the State Security Service.[52] It is a professional interest of an investigative body to achieve prompt results when investigating cases within its competence. Therefore, the State Security Service can influence the agency.

According to the judgment of the Constitutional Court of 14 April 2016, law-enforcement bodies have a professional interest to have as much information as possible as it would simplify the investigation of an already committed crime and contribute to preventing future crimes. A body responsible for conducting investigations is naturally most interested in gathering all the information. Therefore, direct and permanent access of such state bodies to providers of electronic communication services and electronic communication itself greatly increases temptation and risks." The risks of abuse of the powers increase unless there are adequate mechanisms of oversight.[53]

The most important problem dealt with by the court in 2016 remains relevant to this day. Rendering the Operative-Technical Agency subordinate to the State Security Service instead of transforming it into the Operative-Technical Department did not eradicate the risk of arbitrary interference with fundamental rights and freedoms. Naturally, when conducting covert investigative actions which are necessarily based on the relevant statutory provisions, a competent body has to have the power of gathering information in real-time. However, an exclusive mandate for conducting covert investigative actions should not be given to the body, which at the same time is vested with the power to conduct investigative actions. Instead, an independent body should have this power and its activities should be controlled by robust oversight mechanisms.

[48] Available at: https://info.parliament.ge/file/1/BillReviewContent/141415?.
[49] The Law of Georgia on the LEPL Operative-Technical Agency, Article 5.1.
[50] *Ibid.,* Article 3.1.
[51] *Ibid.,,* Article.1.
[52] Order no. 3 of the Prosecutor General of Georgia of 23 August 2019, para. 4.
[53] See judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016, para. 55.

3.1. ELECTION OF THE HEAD OF THE OPERATIVE-TECHNICAL AGENCY

When discussing the safeguards of independence of the agency, it is necessary to discuss the procedure of the election of its head, since the latter has a broad mandate.[54]

The Prime Minister of Georgia appoints and dismisses the head of the agency. A commission especially set up for this purpose submits the candidacy to the Prime Minister. At a glance, the selection procedure provides safeguards for the independence of the agency. However, under the legislation in force, the majority of the commission represents the ruling political party.[55] Furthermore, the majority of the commission is sufficient for electing the candidates. This reduces the likelihood of reaching a politically neutral decision when selecting a candidate to be submitted to the Prime Minister. The participation of a Supreme Court judge and the Ombudsman in the commission's work is only formal.

The special commission is chaired by the Head of the State Security Service. It falls within the exclusive authority of the Head of the State Security Service to submit candidates to the commission. This casts doubts on the independence of the head of the agency from the influence of the State Security Service. The process of selecting candidates by the Head of the State Security Service is also not regulated by law.

In 2017, the then Ombudsman, Ucha Nanuashvili, participated in the special commission set up for the election of the Head of the Operative-Technical Agency. According to him, the Ombudsman's Office received information about the session of the commission a few days earlier; however, no information was supplied concerning the candidates. Despite the fact that the Ombudsman was not in Georgia on the date of the commission's session, which was duly notified to the commission, the Ombudsman was not offered an alternative date to attend the session.

3.2. POWERS OF THE OPERATIVE-TECHNICAL AGENCY

The Operative-Technical Agency is vested with the power to conduct covert investigative actions.[56] Furthermore, the agency, in accordance with the procedure established by law, based on a motion of a competent body for supporting covert surveillance, conducts operative and investigative measures under Article 7.2.a), Article 7.2.b), Article 7.2.e)[57] of the Law of Georgia on Operative and Investigative Activities.[58]

The Operative-Technical Agency will carry out its statutory activities after it is handed a copy of a court order about conducting covert investigative activities;[59] or, in case of emergency, a prosecutor's reasoned resolution.[60]

---

[54] The Law of Georgia on the LEPL Operative-Technical Agency, Article 20.
[55] *Ibid.,* Article 19.2.
[56] The Criminal Procedure Code, Article 3.32.
[57] "A" – interviewing a person; "b" – gathering information and visual observation; "e" examination of objects and documentation.
[58] The Law of Georgia on the LEPL Operative-Technical Agency, Article 8.2.g).
[59] The Criminal Procedure Code, Article 143^3.5.
[60] *Ibid.,* para. 6.

Wiretapping and recording telephone communication are types of covert investigative actions.[61] The agency has exclusive powers[62] to carry out wiretapping and recording of telephone communication performed through common usage of electronic communication networks and means of a competent authority.

In Georgia, wiretapping and recording telephone communications are considered to be some of the greatest threats to the right to respect for private life, as there were numerous instances where illegal telephone recordings were made public.[63] This way, processing personal data affects adversely not only the right to respect for private and family right but also the freedom of expression, freedom of religion and freedom of assembly and association.

The danger arises not only when the Operative-Technical Agency carries out covert wiretapping and recording of telephone conversations but also in situations where it has the exclusive power of "retrieval and recording of information from a communications channel (by connecting to the communication facilities, computer networks, line communications and station devices), the computer system (both directly and remotely) and installation of respective software in the computer system for this purpose."[64]

Before the execution of the 2016 Constitutional Court judgment,[65] the impugned provision of the Law of Georgia on Electronic Communications, provided in express terms for the possibility of installation of a lawful interception system, other devices and software.[66] Despite the declaration of this wording as unconstitutional, the new wording of the law again allows the agency to use the abovementioned mechanism, which directly allows gathering information from any source of communication.

Under the legislation in force, the Operative-Technical Agency has the power of obtaining information in real-time with the use of stationary or semi-stationary technical means and, for this purpose, if necessary, to place without free of charge, a lawful interception management system and/or devices related to it/necessary for its functioning and software.[67] Despite the fact that the legislature allows the possibility of discharging this power only "where necessary", it does not specify its concrete implication and the circumstances where this power can be discharged.

Based on the above-mentioned, the Operative-Technical Agency is authorised to access respective databases of electronic communication companies. The technical protocol and procedures of copying electronic communication identification databases are determined by the normative act of the competent authority.[68] Accordingly, it has the power of obtaining personal information about an individual in real-time through various means (e.g. the use of communications and databases). It is noteworthy that, through the adoption of the normative act, the agency establishes the protocol and terms for this procedure not being subject to any oversight mechanisms, since the "information on the intelligence, counter-intelligence, criminal intelligence and covert investigative activity plans, organisation, logistical support means, forms, methods and results, and information on the

[61] *Ibid.,* Article 143^1 a).

[62] *Ibid.,* Article 3.32.a).

[63] See http://liberali.ge/articles/view/18895/faruli-chanatserebi--gadauchreli-problema [accessed 04.09.2020].

[64] The Criminal Procedure Code, Article 3.33 and Article 3.34.

[65] See judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016.

[66] The Law of Georgia on Electronic Communications, Article 8^3, see Law of Georgia no. 480 of 22 March 2017.

[67] The Law of Georgia on Electronic Communications, Article 8^1.1.a).

[68] The Law of Georgia on Electronic Communications, Article 8^3.2.

planning, implementation and financing of specific measures and programmes" falls within the category of state secrets.[69]

Within the framework of covert investigative actions, the Operative-Technical Agency is also authorised to install respective devices and software to obtain information in real-time from communication lines. This authorisation has been vested with the agency in terms of the following covert investigative actions: wiretapping and recording telephone communication; retrieval and recording of information from communication channels (by connecting to the communication means, computer networks, line communications and station devices), the computer system (both directly and remotely) and installation of respective software in the computer system for this purpose and determining geolocation in real-time.[70]

Before the execution of the Constitutional Court Judgment (no. 1/1/625,640), the Operative-Technical Department of the State Security Service was in charge of carrying out covert investigative actions instead of the Operative-Technical Agency.[71] The Constitutional Court examined the scope of the powers of the State Security Service (technical possibilities, their placement, administration and direct use for obtaining information in real-time) in terms of assessing the actual risk of abuse and thus the violation of human rights.[72]

The existence of a legitimate reason for interfering with a constitutional right – interests of the investigation, prevention of a crime, protection of the rights of others – does not imply a state's power to discharge its authority in an unlimited and control-free manner. "The Constitution demands that interference with a constitutional right for this interest should be allowed only in exceptional cases when other legitimate means of protecting this interest have been exhausted, in the least intrusive and proportionate way".[73]

The Constitutional Court observed in its judgment that the lawful interception management system is the most effective means for the surveillance of telephone conversations since it allows direct and direct and immediate control of almost all telephone conversation and obtaining any information in real-time that is exchanged through this communication. This was confirmed by the representative of the state security service during the examination of the merits.[74]

Vesting the State Security Service with full powers in this regard against the background of weak oversight mechanisms was considered to be unconstitutional by the Constitutional Court.[75] Despite this, since the legislative changes effected by the Parliament of Georgia on 22 March 2017, the failure to create appropriate safeguard mechanisms against unjustified and unlimited interferences and practical independence of the Operative-Technical Agency from the State Security Service and the problems mentioned above remain relevant.

The statistics published on the website of the Supreme Court of Georgia demonstrates that there is an increase in the number of motions for covert investigative actions.[76] In 2015, out of 362 motions

[69] The Law of Georgia on State Secret, Article 6.d).
[70] The Criminal Procedure Code, Article 143^3.4.
[71] The Criminal Procedure Code, Article 3.32, the version in force as of 08/02/2017.
[72] Judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016, para. 39.
[73] *Ibid.,* 40.
[74] *Ibid.,* 49.
[75] Judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016. The full version is available at: https://matsne.gov.ge/ka/document/view/3263731?publication=0.
[76] See the statistical data published by the Supreme Court of Georgia, http://www.supremecourt.ge/statistics/.

filed with the court, all except for 61 motions were upheld; in 2016, out of 401 motions only 56 were rejected; in 2017, out of 548 motions submitted, 27 were rejected; in 2018, out of 1,059 motions, only 78 were rejected; and in 2019, out of 1,037 motions, 133 were rejected. It is clear that the number of motions submitted to the courts increases annually and the number of rejected motions decreases. It naturally gives rise to misgivings that law-enforcement authorities interfere in private life too much.

3.3. COPYING ELECTRONIC COMMUNICATION IDENTIFICATION DATABASES BY COMPETENT AUTHORITIES

The legislation in force determines the possibility of the Operative-Technical Agency to create the Central Identification Data Repository (CIDR) of Electronic Communications.[77] The Operative-Technical Agency is also authorised to copy electronic communication identification databases and retain them in the CIDR of Electronic Communications with an electronic control system.[78] While the legislation determines in express terms the group of persons concerning whom covert investigative actions can be used,[79] this provision does not specify *whose data exactly can the agency copy and retain.* Therefore, there is a risk that this action will be conducted concerning not only the persons falling within the category determined by law but other persons as well (and the data can be copied to the so-called "alternative bank" to circumvent oversight).

The Constitutional Court observed in its judgment of 14 April 2016 that, according to the representative of the State Security Service, it is technically possible to copy and retain identification data into the so-called "alternative bank" so that nobody would be aware of this database and even the Personal Data Protection Inspector would not have access to it. Therefore, the representative did not exclude the possibility of situations where pieces of information are separated from each other and some of them are stored in the alternative database. This would allow the agency and thus the service to control any person and monitor social relations. Stemming from the fact that there can be no oversight of this process and the terms of retention of data cannot be monitored, there will be no impediments in terms of an oversight mechanism concerning gathering information about any person, copying and retaining data.

Retention of information by a competent authority can have a legitimate aim, i.e., protection of public safety and the rights of others. Under the legislation in force, "the body carrying out covert investigative actions, also investigative authorities or persons, shall be obliged, within their powers, to limit, *as much as possible*, the monitoring of communications and persons that are not related to the investigation."[80] Stemming from the objective of the Operative-Technical Agency, it is possible to assume that the regulation about copying data only concerns the object of a covert investigative action. However, this wording is too general and allows extensive interpretation. It is, therefore, imperative to specify by legislation that this action does not concern a person who had no link with investigative actions.

Under the precedent established by the Court of Justice of the European Union (CJEU), the EU directive on Privacy and Electronic Communications, under which communication providers were

[77] The Law of Georgia on the LEPL Operative-Technical Agency, Article 11.
[78] The Law of Georgia on Electronic Communications, Article 8^3.
[79] The Criminal Procedure Code, Article 143^3.2.b).
[80] The Criminal Procedure Code, Article 143^7.1.

obliged to retain communication data for supplying to law-enforcement agencies, was incompatible with the right to respect for private life.[81]

As regards the duration of retention of obtained data, the agency is authorised to retain electronic communication identification data for no more than 12 months. However, in the cases of specific circumstances, this term can be extended for no more than another three months. [82]

Before the judgment of 14 April 2016, the law provided for a two-year term. However, the provision[83] laying down this term was declared unconstitutional. The Constitutional Court held that "the degree of the interference is reasonably increasing proportionally in terms of the duration of the interference. [84] Therefore, the Constitutional Court ruled that the specific provision laying down this term was against the Constitution of Georgia. [85]

3.4. COMPATIBILITY OF THE LEGISLATION GOVERNING THE OPERATIVE-TECHNICAL AGENCY WITH INTERNATIONAL STANDARDS

The Constitutional Court in its judgment of 14 April 2016 observed the following:

a) Direct and permanent access of state bodies vested with investigative powers to the data stored with the providers of electronic communication services and the electronic communication greatly increased, based on the interests of the investigation, the temptation and risk of arbitrary interference with the right.[86]

b) The existing legislative mechanisms failed to exclude the possibility of circumventing the Personal Data Protection Inspector and thus the risk of wiretapping telephone communication without a court order.

Despite the criticism of the Constitutional Court, the legislation in force maintains to this day the agency's direct access to electronic communication. Therefore, the possibility of abuse of this technical possibility on the part of the service remains realistic.

It is noteworthy that the legislation of the Russian Federation contains a similar regulation (the system of covert surveillance giving security services and police technical the possibility to circumvent the authorisation procedure and access communication means without a prior court order). In its judgment of 4 December 2015, the Grand Chamber of the European Court of Human Rights held that a system, which enables the secret services and the police to directly intercept the communications of each citizen without requiring them to show an interception authorisation to the communications service provider, or anyone else, is particularly prone to abuse.[87]

---

[81] Democratic and effective oversight of national security services, p. 23, see Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, see in particular [29] [57] [58] and [65].
[82] The Law of Georgia on the LEPL Operative-Technical Agency, Article 15.1 and Article 15.2.
[83] The provision governing retention of the data for two years is contained in the Law of Georgia on Electronic Communications, Article 8^3.1.
[84] See judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016, para 108.
[85] *Ibid.,* para. 113.
[86] Judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016, para. 55.
[87] *Roman Zakharov v. Russia*, application no. 47143/06, judgment of the Grand Chamber of the European Court of Human Rights of 4 December 2015, para. 270.

The functioning of the system of accessing means of communication and covert surveillance is differently regulated in the countries studied by us. To limit the possibilities of arbitrary use of intrusive measures, the procedure of the use of covert investigative actions, their need and proportionality are regulated in detail by legislation. Furthermore, the control (both executive and judicial), as well as the adequate and coordinated functioning of oversight mechanisms, is of great significance.[88]

Canada – the Canadian legislation obliges the Intelligence Service in imperative terms to conduct covert investigative actions based on a court order. A motion should contain the facts relied on to justify the belief, on reasonable grounds, that a warrant under this section is required to enable the service to investigate a threat to the security of Canada, the type of communication proposed to be intercepted, and the identity of the person, if known, whose communication is proposed to be intercepted. The motion should also indicate the period for which the warrant is requested.[89]

Norway – In Norway, police and security services can resort to communication surveillance, recording and other surveillance measures upon a court's order if it is reasonably believed that a person has committed or may commit a crime punishable for a term of ten years or more.[90] In case of emergency, it is also possible to conduct, under a prosecutorial instruction, these investigative actions without a court order. The legality of an investigation action should be approved by a judge within 24 hours from the start of the measure.[91] The respective body of the Norwegian Post and Telecommunications Authority must be notified about this measure unless it is an exceptional case.[92]

Latvia - in Latvia, computer-related operative investigative actions can be carried out by investigative authorities, among others, the Constitutional Security Bureau, the Security Police and the Military Intelligence and Security Services.[93] Service providers are obliged by law to retain identifying electronic communication data for 18 months.[94] The service providers make these data available for competent investigation authorities upon their request in accordance with the procedure established by law. The service providers send information to the Personal Data State Inspector annually. The latter processes these data within two months and sends them to the European Commission.[95]

[88] DCAF Parliamentary Brief Safeguards in Electronic Surveillance, p. 4, available at: https://www.dcaf.ch/dcaf-parliamentary-brief-safeguards-electronic-surveillance.

[89] The Canadian Security Intelligence Service Act, article 21.

[90] Norway, the Criminal Procedure Act, section 216 a.

[91] Norway, the Criminal Procedure Act, section 216 d.

[92] Norway, the Electronic Communications Act, Section 6-2a.

[93] Latvian Centre for Human Rights, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, 2015, p.1.

[94] Latvia Electronic Communications Law Section 19 (11).

[95] Latvia Electronic Communications Law Section 71^1 (5).

4. PROCEDURAL SAFEGUARDS RELATED TO COVERT INVESTIGATIVE ACTIONS

4.1 PROCEDURE OF RETENTION AND DESTRUCTION OF INFORMATION GATHERED FROM COVERT INVESTIGATIVE ACTIONS

The law should exhaustively govern the safeguards related to the retention and destruction of information obtained during covert investigative actions.[96]

Under the legislation in force, both the body in charge of covert investigative actions and the respective investigative body are responsible for adequate retention and protection of information obtained through covert investigative actions.[97] In those cases where this information is included in the case-files as material evidence, it will be retained for the period of the retention of these criminal case-files. After the expiry of this term, the case-files will be immediately destroyed by the judge or by a judge of that court who, or the judge of which, made a decision on conducting the covert investigative action or recognised as lawful or unlawful the covert investigative action that was carried out without a court order in the case of urgency.

The Criminal Procedure Code governs differently those cases where the information obtained does not have probative value for the investigation or the information obtained as a result of the covert investigative action that has been carried out without the order of a judge in the case of urgency and that, even though recognised by a court as lawful, has not been submitted as evidence by the prosecution. Such information will be immediately destroyed after the termination or completion of such actions. Such information is destroyed by a prosecutor providing procedural supervision over the investigation of the given case, or supporting the state prosecution or by their superior prosecutor, in the presence of the judge, or a judge of from the same court, who made the decision on conducting this covert investigative action, or recognised as lawful or unlawful the covert investigative action carried out without a court order in the case of urgency. [98]

Operative and investigative activities imply using covert methods along with overt methods.[99] Therefore, it is imperative to have safeguards concerning the destruction of information in place. This is moreover significant in the circumstances where the information obtained through such measures concerns an individual's private life and related to the crime at stake. Despite this, the Law of Georgia on the LEPL Operative and Investigative Activities does not specify the body responsible for the destruction of this information and is limited to supplying information to the Prosecutor General of Georgia and the court.[100] Similarly, the law does not determine the procedure for the destruction of the information. In the case of *Iordachi v. Moldova*,[101] the European Court of Human Rights observed that the legislation in force should determine the procedure for the destruction of information obtained through covert methods. The Court ruled that the failure to comply with this obligation amounted to the violation of Article 8 of the Convention.[102]

---

[96] Review of the Case-Law of the European Court of Human Rights and the Constitutional Court of Georgia, the Right to Respect for Private Life and State's Obligations, p. 200, 2017.
[97] The Criminal Procedure Code, Article 143^5.1.
[98] *Ibid.,* Article 143^8.1, 143^8.3, 143^8.5 and 143^8.6,
[99] The Law of Georgia on Operative and Investigative Activities, Article 1.1.
[100] *Ibid.,* Article 6.4.
[101] *Iordachi v. Moldova*, application no. 25198/02, judgment of the European Court of Human Rights of 2009.
[102] Review of the Case-Law of the European Court of Human Rights and the Constitutional Court of Georgia, the Right to Respect for Private Life and State's Obligations, 2017, p. 201.

4.2 OBJECTS OF COVERT INVESTIGATIVE ACTIONS AND THE LEGAL SAFEGUARDS FOR THEIR PROTECTION

An object of covert investigative actions is a person against whom such measures are carried out.[103] Under the Criminal Procedure Code of Georgia, there is a reasonable cause to believe that a person against whom a covert investigative action is to be carried out has committed any of the crimes provided for by sub-paragraph (a) of Article 143³.2 (person directly related to the crime), or a person receives or transmits information that is intended for, or is provided by, a person directly related to the crime, or a person directly related to the crime uses the communication means of the person.[104]

Communications data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[105] Under Article 13 of the Convention for the Protection of Human Rights and Fundamental Freedoms, everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

A person, against whom a covert investigative action has been carried out, shall be notified in writing about the action as well as of the contents of the materials obtained as a result of that action and the destruction of the above material. Along with that information, that person shall also be presented with a court order on conducting covert investigative actions against him/her as well as the materials based on which the judge rendered such a decision.[106] The legislation in force before 1 August 2014 did not contain the duty of written notification of objects of covert investigative actions.[107] The introduction of such regulations is commendable; however, the respective provisions are obscure.

"A decision as to the time when a person is to be notified about conducting covert investigative actions against him/her and be handed over the relevant order and materials shall be made by the prosecutor, both during and after the legal proceedings, taking into account the interest of the legal proceedings."[108] The prosecutor has a statutory power not to notify a person about conducting covert investigative actions against him/her within 12 months. The court issues a permit only in case of extension of this term for another 12 months.[109] Stemming from the fact that it is completely possible that the material that was destroyed had been obtained through a serious violation of human rights,[110] objects of covert investigative actions must enjoy prompt and effective legal remedies for the breached rights. It is, therefore, recommended that the judge, when allowing covert investigative actions, determines the date of notification thus determining when a person concerned must be notified about the investigative measures conducted against him/her. Notification of a person that covert investigative actions have been conducted concerning him/her

[103] The Criminal Procedure Code, Article 3.31.
[104] *Ibid.*, Article 143³.2.b).
[105] Democratic and effective oversight of national security services, p. 23, See *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others*, [29] [57] [58] and [65].
[106] The Criminal Procedure Code, Article 143⁹.3.
[107] See the Criminal Procedure Code, in force before 01.08.2014.
[108] The Criminal Procedure Code, Article 143⁹.3.
[109] *Ibid.,* para. 4.
[110] *Ibid.,* Article 143⁸.1.

is of central importance, since challenging such actions are usually hampered by the fact that persons concerned are not even aware of the violation of their rights.[111]

The code offers different regulations for those cases where a person learns about the execution of a covert investigative action against him/her during legal proceedings. The person concerned is entitled to a one-time appeal of the court order authorising a covert investigative action to the investigation panel of the relevant court of appeal within 48 hours after the receipt of the above information and being informed of the right to appeal the order.[112] The non-appearance of the appellant and the prosecution does not preclude the review of the appeal.[113]

Accordingly, the person concerned can only challenge the court order and not the use of particular methods of surveillance by the Operative-Technical Agency.[114] This cannot be deemed to be an effective remedy for the violation of a human right.

[111] Venice Commission, 2007, § 243.
[112] The Criminal Procedure Code, Article 143^3.14.
[113] *Ibid.,* Article 143^3.16.
[114] The State Inspector's Service is authorised to inspect the above-mentioned.

5. SIGNIFICANCE OF A COURT ORDER ON COVERT INVESTIGATIVE ACTIONS

Often, authorisation is considered to be the best mechanism for the protection of human rights.[115] According to the legislation in force, in Georgia, covert investigative actions can be carried out only based on a court order. A judge of a district (city) court must render an order upon a prosecutor's reasoned motion, except in the case of urgency. However, the court also takes a decision about the legality of a covert investigative action conducted in the case of urgency. [116] A court order is also necessary when operative and investigative measures are conducted using covert methods.[117]

The Venice Commission highlights the importance of the qualifications and independence of judges in the process of issuing permission for conducting a covert investigative action.[118] According to the best international practice, a court order is issued by a specially appointed judge with appropriate training. For instance, in Hungary, it is a judge appointed by the President of the Metropolitan Court.[119] In Latvia, permissions for covert investigative actions[120] are given by specially trained judges[121] (investigative judges) appointed by the President of a District (City) Court.[122]

The Georgian Procedure Code allows a judge to examine a prosecutor's motion without an oral hearing.[123] However, some countries provide for application hearings where complex issues arise or a judge wishes to question a security service representative. In this process, a judge has the possibility of receiving all the necessary information from the relevant official to reach a decision.[124] It is desirable that the Georgian legislation follows this approach.

[115] Democratic and effective oversight of national security services, p. 55.
[116] The Criminal Procedure Code, Article $143^{3.}1$ and $143^{3}.6$
[117] The Criminal Procedure Code, Article 33.6.e).
[118] Venice Commission, Report on the Democratic Oversight of the Security Services, 2007. 205-206
[119] Democratic and effective oversight of national security services, p. 54.
[120] The Criminal Procedure Law, Latvia, Section 212; 21.11.2019.
[121] The Court Administration Judicial System in Latvia, p. 22.
[122] The Criminal Procedure Law, Latvia, Section 40; 21.11.2019.
[123] The Criminal Procedure Code, Article 143^{3}.
[124] Democratic and effective oversight of national security services, p. 55.

6. THE ROLE OF THE STATE INSPECTOR'S SERVICE IN CONDUCTING COVERT INVESTIGATIVE ACTIONS

The legislative regulations governing covert investigative actions are not sufficient on their own for preventing disproportional restriction of the right to respect for private life. It is also imperative to have adequate mechanisms of oversight in place, especially in those conditions where covert investigative actions are carried out by the Operative-Technical Agency vested with broad powers and subordinate to the State Security Service.[125]

In conducting covert investigative actions, it is essential to maintain a fair balance between the interest of crime investigation and the inviolability of the individual's personal space.[126] In Georgia, according to the current legislation, this is controlled by the State Inspector's Service.[127]

The Institute of the State Inspector has existed in Georgia since 2013 in various forms, functions and names. In recent years, the State Inspector's Service has undergone significant changes. Adopted in 2018, the Law of Georgia on the State Inspector's Service equips the service with the oversight power over the investigation, legality of data processing, covert investigative actions and the activities carried out at the CIDR of Electronic Communications. A number of norms came into force in 2019 when the Office of the Personal Data Protection Inspector was abolished and replaced by the State Inspector's Service.

6.1. THE STATE INSPECTOR'S SERVICE AS A SUPERVISORY BODY

The procedure of conducting covert investigative actions is governed by the Criminal Procedure Code. Under the Code of Criminal Procedure, it is imperative to deliver immediately, not later than 48 hours, a copy in a tangible (documentary) form containing only requisites and an operative part of the ruling authorising a covert investigative action to the State Inspector's Service.[128] The Criminal Procedure Code provides for a distinct regulation for the cases where covert wiretapping and recording of telephone conversations are conducted based on a court's order. A judge's order, which contains only requisites and an operative part, granting authorisation to carry out covert wiretapping and recording of telephone conversations, is delivered by the Agency upon its receipt to the State Inspector's Service as an electronic copy through an electronic control system. Upon the confirmation of the electronic delivery of an electronic copy of the judge's order to the State Inspector's Service, the agency commences the covert investigative action.[129]

The Criminal Procedure Code regulates the cases of urgency differently when a delay may result in the destruction of the factual data important for the criminal case (investigation) or make it impossible to gather this data. "In the case of urgency, a resolution of a prosecutor on carrying out a covert investigative action, which contains only requisites and an operative part, not later than 12 hours from the time of commencing the covert investigative action specified in the resolution,

[125] The Criminal Procedure Code, Article 2.32.
[126] See the 2017 Report on the Situation of the Protection of Personal Data and Inspector's Activities, p. 53, available at: https://personaldata.ge/cdn/2018/12/angarishi_2017.pdf.
[127] The Law of Georgia on the State Inspector's Service, Chapter IV.
[128] The Criminal Procedure Code, Article $143^{3}.5$.
[129] *Ibid.,* para. 5^{1}.

shall be submitted to the State Inspector's Service by the prosecutor or an investigator by order of the prosecutor in a tangible (documentary) form."[130]

The Criminal Procedure Code provides for a distinct regulation for the cases where covert wiretapping and recording of telephone conversations are conducted in the case of urgency. A resolution of a prosecutor on carrying out this covert investigative action, which contains only requisites and an operative part, is delivered by the agency upon receipt to the State Inspector's Service as an electronic copy through an electronic control system. Upon the confirmation of the electronic delivery of an electronic copy of the resolution of the prosecutor, the agency shall commence the covert investigative action.[131]

However, there are frequent occurrences in practice where a court order is not delivered to the State Inspector or delivered late. For instance, during the reporting period, notably in 2016, the inspection demonstrated that in six cases a copy of the decision had not been delivered to the inspector at all. The Prosecutor General referred to the shortage of time and conducing several covert investigative actions as reasons for the delay. In three cases, resolutions adopted in the case of urgency were submitted to the inspector with a five-day delay, when virtually all investigative actions had been already fully conducted.[132] Conducting covert investigative actions without the supervision of the State Inspector increases the risks of unjustified interference with human rights. Therefore, the legislation should provide for proper safeguards against such risks, among others, responsibility should be determined for the failure to comply with the statutory duties.

6.1.1. GROUNDS FOR SUSPENDING COVERT INVESTIGATIVE ACTIONS

The State Inspector's Service has the power to suspend a covert investigative action through an electronic control system. This power can be exercised when a court order or a copy of the prosecutor's resolution in a tangible (documentary) form is not available and requisites and/or the operative part of the prosecutor's resolution submitted through an electronic system or in a tangible (documentary) form contain ambiguities or inaccuracies or fail to coincide with each other.[133] If the grounds for suspending a covert investigative action are not removed within three days after it was suspended, a state body with an appropriate authority shall terminate the covert investigative action upon the expiry of the statutory period.[134] The material obtained from the covert investigative action concerned is destroyed.[135] As regards the removal of the grounds for suspension, they are laid down in Article 143^6 of the Criminal Procedure Code.

The above power was given to the State Inspector's Service after the abolition of the two-stage electronic system as a result of the Constitutional Court's judgment on 14 April 2016.

According to the State Inspector's 2017 annual report, since April 2017, this mechanism has been used with regard to 21 court order/prosecutorial resolution. Out of them, 10 contained ambiguities/inaccuracies. As a result of the removal of the grounds for suspension, all covert

[130] *Ibid.,* Article $143^3.6^2$.
[131] *Ibid.*
[132] The 2016 Report on the Situation of the Protection of Personal Data and Inspector's Activities, pp. 65-66.
[133] The Criminal Procedure Code, Article $143^6.5$.
[134] *Ibid.,* para. 3.
[135] *Ibid.,* para. 16.

investigative actions were resumed.[136] In total, in 2017, the State Inspector's Service received 699 court orders about partially upholding or rejecting motions for starting, continuing, confirming covert wiretapping and recording of telephone conversations.[137] As regards 2018, the State Inspector, out of the 1,397 court orders received concerning telephone conversations, suspended the covert investigative action in 96 cases.[138] In 2019, the suspension mechanism was used in 98 court orders/prosecutorial resolutions. The State Inspector's Service received 1,362 court orders that year.[139]

6.1.2. THE STATE INSPECTOR'S PARTICIPATION IN THE DESTRUCTION OF THE INFORMATION OBTAINED FROM COVERT INVESTIGATIVE ACTIONS

Information obtained through covert investigative actions, that has no value for the investigation, must be destroyed by the decision of the prosecutor. Also, the information obtained as a result of the covert investigative action that has been carried out without the order of a judge in the case of urgency and that, even though recognised by a court as lawful, has not been submitted as evidence by the prosecution in the manner prescribed by Article 83 to the court that hears the case on the merits. The materials must be immediately destroyed if they are obtained as a result of operative-investigative actions and do not concern a person's criminal activities but include details of that person's or any other person's private life and are subject to destruction. The information obtained as a result of covert investigative actions shall be destroyed in the presence of a judge by a prosecutor providing procedural supervision over the investigation of the given case or supporting the state prosecution or by their superior prosecutor. A record of the destruction of materials obtained as a result of covert investigative actions, signed by the relevant prosecutors and judges shall be forwarded to the State Inspector's Service.[140]

As regards the material obtained from covert investigative actions, that is not admitted as evidence by the court, it will be destroyed immediately after the elapse of 6 months since the adoption of the final judgment in the case. The State Inspector's Service is not informed about this,[141] which should be redeemed. It is recommended to inform the State Inspector's Service about the destruction of the material containing personal data obtained from covert investigative actions; this data should be destroyed in the presence of a representative of the State Inspector's Service or a judge (if the case falls within the jurisdiction of the State Inspector's Service).

6.1.3. OTHER MECHANISMS OF OVERSIGHT AT THE DISPOSAL OF THE STATE INSPECTOR, INSPECTION

In the process of wiretapping and recording telephone communications (except for covert investigative actions carried out within investigation led by the State Inspector's Service) the following are controlled by the State Security Service: legality of data processing through electronic

[136] See the 2017 Report on the Situation of the Protection of Personal Data and Inspector's Activities, p. 56, available at: https://personaldata.ge/cdn/2018/12/angarishi_2017.pdf.
[137] See the 2018 Report on the Situation of the Protection of Personal Data and Inspector's Activities, p. 55, available at: https://personaldata.ge/cdn/2018/12/angarishi_2017.pdf.
[138] See the 2017 Report on the Situation of the Protection of Personal Data and Inspector's Activities, p. 71.
[139] See the 2019 Report on the State Inspector's Activities, p. 94.
[140] The Criminal Procedure Code, Article 143[8].
[141] *Ibid.*

system of control; legality of data processing through a special electronic system of control; legality of processing data by a person processing data/authorised official (inspection).[142]

The Operative-Technical Agency has the power to create and, in accordance with the procedure established by law, use technical, hardware and software means necessary for carrying out respective actions.[143] However, the legislation in force does not ensure safeguards against the abuse of its powers by the agency. Furthermore, it is unclear which particular device at what time will be installed by the agency. At such times, the State Inspector's Service is devoid of any possibility of carrying out oversight.[144] The agency also has the possibility of obtaining communication data in real-time.[145] Therefore, the agency can freely carry out covert wiretapping and uncontrolled collection of data thus infringing not only the rights of an object of covert investigative actions but also those of third persons.

The State Inspector's Service carries out inspection (inspection of the legality of data processing is implied) through supervision of covert investigative actions – in the cases under Article 143[1].1.a)-f) of the Criminal Procedure Code – and also through controlling the activities carried out in the central bank of electronic communication identification data and inspection of the legality of data processing (inspection).

According to the actual legislation, the State Inspector's Service is only authorised to inspect the legality of data processing.[146] When conducting the inspection, the State Inspector is authorised "to obtain information about the technical infrastructure used for covert investigative actions and inspect this infrastructure".[147] However, it is unclear what type of infrastructure is accessible and what methods have been used. The statute of the State Inspector's Service is also reticent about this issue. The annual reports of the State Inspector's Service also omit the information about the inspection of technical infrastructure by the inspector.

The Constitutional Court observed in its judgment of 14 April 2016 that following factors can ensure the effectiveness of inspection: the first is "complete distancing of the inspector from the process" (this can be assumed to be present partially by virtue of the abolishment of the two-state electronic system) and the second is "when it is possible to compare the State Security Service's information with information obtained from other sources." For instance, when the inspector can compare information supplied by an independent body or even communication company with the information submitted by the State Security Service.[148] The problem of obtaining information from various sources remains problematic to this day.

Another fact casting doubts on the proper discharge of powers by the State Inspector's Service is that the agency is authorised to copy and retain electronic communication identification data in

[142] The Law of Georgia on the State Inspector's Service, Article 18.
[143] The Law of Georgia on the LEPL Operative-Technical Agency, Article 8.2.c).
[144] One of the issues of the constitutional complaint filed with the Constitutional Court in 2015 concerned the alleged unconstitutionality of vesting the Operative-Technical Department with this power. However, the Operative-Technical Agency maintained this mandate to this day. See judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016.
[145] The Law of Georgia on the LEPL Operative-Technical Agency, Article 9.
[146] The Law of Georgia on the State Inspector's Service, Article 2.a).
[147] *Ibid.*, Article 18.7.c).
[148] See judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016, para. 65.

the CIDR of Electronic Communications.[149] The legislature does not specify which data this can be and, accordingly, there is a risk of copying and retaining information to the alternative bank of data beyond the scope allowed by a court order.

According to the 2019 annual report of the State Inspector, 156 inspections were carried out in the course of the year. Out of which, only 29% of inspections were carried out by the service's initiative and the rest were conducted based on applications and notification.[150] Under the initiative of the State Inspector's Service, within the oversight of covert investigative actions, the Operative-Technical Agency was inspected only six times.[151] It is not clear from the report what particular violations were identified, what recommendations were made and what were the methods employed in the inspection. It is natural that identifying three violations by the Operative-Technical Agency out of six inspections is noteworthy and demands for more inspections to be carried out annually.

According to the 2019 annual report of the State Inspector's Service, similar to the previous years, the number of files received by the service is on the increase.[152]

Stemming from the abovementioned, it is desirable to introduce a mandatory minimum number of inspections of the Operative-Technical Agency, including other bodies related to covert investigative actions, to be carried out annually by the State Inspector's Service. The State Inspector's Service should provide for information in its annual reports about the methods of inspection used and the outcomes of the inspections; the concrete recommendations made and how they were fulfilled. The data should be processed only to the extent necessary for achieving a specific legitimate aim. Therefore, it is of vital importance that the State Inspector's Service used the mechanism of inspection effectively.

6.1.4. INSPECTION OF GATHERING INFORMATION FROM CYBERSPACE

The Operative-Technical Agency is authorised to obtain information in real-time within covert investigative actions through stationary, semi-stationary or non-stationary technical means. This also implies obtaining information from cyberspace.[153] As mentioned above, the agency also enjoys the power of copying and retaining electronic communication identification databases.

In its judgment of 14 April 2016, the Constitutional Court discussed problems related to obtaining information from cyberspace in real-time and the associated dangers of uncontrolled interference in a person's personal space.

Presently, only the inspection mechanism can be applied to processing the data obtained from cyberspace.[154] The electronic control system cannot monitor this activity. However, it is a fact that, due to the intensive use of this mechanism and accordingly the volume of the respective information, the data obtained from cyberspace gives far more information about a person's private

[149] The Law of Georgia on Electronic Communications, Article 8^3; the Law of Georgia on the LEPL Operative-Technical Agency, Article 11.
[150] The 2019 Report on the State Inspector's Activities, p. 36
[151] *Ibid.,* p. 96.
[152] The 2019 Report on the State Inspector's Activities, p. 35.
[153] The Law of Georgia on the LEPL Operative-Technical Agency, Article 9.6; the Criminal Procedure Code, Article 3.32.
[154] The Law of Georgia on the State Inspector's Service, Article 18.3.

life. Therefore, uncontrolled intrusion in this space may result in more intensive interference with and, therefore, violation of fundamental human rights.[155]

The Operative-Technical Agency's access to information in cyberspace for conducting covert investigative actions with limited oversight mechanisms of the State Inspector increases the risks of infringement of human rights especially in those circumstances where the inspection mechanism is ridden with a number of problems.

6.2. THE STATE INSPECTOR'S SERVICE AS AN INVESTIGATIVE BODY

Since 2019, the State Inspector's Service has been vested with the power to investigate[156] operative and investigative activities. [157]

Investigative jurisdiction of the State Inspector's Service applies to the crimes provided for by Articles 144^1–144^3, Article 332(3)(b) and (c), Article 333(3)(b) and (c), Article 335 and/or Article 378(2) of the Criminal Code of Georgia cover the crimes committed by the representatives of law enforcement bodies, officers or persons equal to them. They also cover other crimes committed by the representatives of a law enforcement body, officers or persons equal to them which caused the death of a person while this person was in a temporary detention isolator or a penitentiary institution or any other place which he/she was forbidden to leave against his/her will by a representative of a law enforcement body, an officer or a person equal to him/her, and/or this person was otherwise under the effective control of the state.[158]

The DRI applied to the State Inspector's Service and requested public information about the cases falling within the jurisdiction of the service. According to the service's response, from 1 November 2019 to 1 April 2020, the investigative department of the service instituted investigation in 131 cases, out of which 118 concerned crimes were allegedly committed by the officials of the Ministry of Internal Affairs of Georgia. 120 cases out of 131 cases were instituted concerning abuse of official powers with the use of violence or firearms. It is noteworthy that, in this period, the Investigative Department of the State Inspector's Service instituted a prosecution against only one person in one criminal case out of all the cases.[159]

It was mentioned several times that the State Inspector's Service supervises the Operative-Technical Agency[160] and the agency has the exclusive power to conduct covert investigative actions under Article 143^1.1.a)-d) of the Criminal Procedure Code. Accordingly, concerning the State Inspector's cases, covert investigative actions are carried out by the very agency, which is supervised (unless a particular case is not within its jurisdiction) by the State Inspector's Service itself. Accordingly, the State Inspector's Service is vested with two completely distinct powers, viz., on the one hand, to protect a person's private life, assess and eradicate risks of unjustified interference in an individual's private space from respective bodies or officials and, on the other hand, to conduct investigative actions, thus possibly contributing to illegal interference in an individual's personal space.

[155] See Judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016, para. 78.
[156] The Law of Georgia on the State Inspector's Service, Article 2.c).
[157] *Ibid.,* Article 20.a).
[158] The Law of Georgia on the State Inspector's Service, Article 19.1.
[159] See Letter no. SIS 5 20 00005180 of the State Inspector's Service.
[160] The Law of Georgia on the State Inspector's Service, Article 18.

The Criminal Procedure Code is familiar with the institute of a supervising judge, who for the purposes of Chapter XVI[1] of this code, supervises covert investigative actions carried out concerning crimes falling within the jurisdiction of the State Inspector's Service.[161]

According to the actual legislation, a supervisory judge replaces the State Inspector's Service and assumes almost all its powers (in terms of the oversight of the Operative-Technical Agency) where covert investigative actions are conducted in relation to a crime falling within the State Inspector's Service.[162] At the same time, concerning criminal proceedings conducted by the State Inspector's Service, a supervising judge controls the carrying out of a covert investigative action under Article 143[1].1.(a) of the Criminal Procedure Code using a stationary technical means with an electronic control system and a special electronic control system.[163] At the first glance, vesting a supervisory judge with this power is commendable as there are more oversight mechanisms effected by the court over covert investigative actions. However, the introduction of this mechanism does not create a strong safeguard against interference with human rights and fundamental freedoms.

A supervising judge supervises covert investigative actions such as wiretapping and recording telephone conversations and the activities carried out at CIDR of Electronic Communication with an electronic control system.[164] Therefore, the following covert investigative actions can be left beyond this supervision and give rise to uncontrolled interference in a person's personal space: the retrieval and recording of information from a communications channel (by connecting to the communication facilities, computer networks, line communications and station devices), the computer system (both directly and remotely) and installation of respective software in the computer system for this purpose; the monitoring of a postal and telegraphic transfer (except for diplomatic mail); video and/or audio recording, photographing; and electronic surveillance through technical means the use of which does not cause harm to human life, health and the environment.

It should also be mentioned that judicial control effected by the supervisory judge over the covert investigative actions carried out regarding the cases falling within the jurisdiction of the State Inspector's Service creates certain chaos. There is no uniform protection standard that would make an individual's sense of stability and security. The following can be used as an example: "in those cases, where after the institution of the investigation, it is established that the investigation of the criminal case falls within the jurisdiction of the State Inspector's Service, after the completion of urgent investigative actions, the prosecutor refers the case immediately according to the jurisdiction."[165] At the same time, in the case of urgency, under a prosecutorial resolution, covert investigative actions can be started and, accordingly, the State Inspector's Service supervises the activities carried out by the Operative-Technical Agency. After the case is referred to the State Inspector's Service, the supervision is carried out by a supervising judge.

From 1 November 2019 to 1 April 2020, 3 criminal cases were referred to the Investigative Department of the State Inspector's Service. Besides, structural units of the prosecutor's office referred 2 criminal cases to the State Inspector's Service according to the rules of official and territorial jurisdiction.[166]

---

[161] The Criminal Procedure Code, Article 3.32[1].
[162] *Ibid.*, Article 1433, paras. 5, 56 (b), 57 , 58 , 59 , 64 , 7.
[163] *Ibid.,* Article 143[4].3.
[164] *Ibid.,* Article 3.32[1].
[165] See the Law of Georgia on the State Inspector's Service, Article 19.2.
[166] Letter no. SIS 5 20 00005180 of the State Inspector's Service.

The problem of redistribution of functions in this way is made even more obvious by the fact that the investigative actions conducted by the State Inspector's Service is managed and supervised by a respective structural unit of the Office of the Prosecutor General and, in those cases where a crime is allegedly committed by an official of the Office of the Prosecutor General, the management and supervision are effected by the Inspection General of the Office of the Prosecutor General. At the same time, all other investigative actions (which are certainly managed and supervised by the Office of the Prosecutor General) are supervised by the State Inspector's Service itself. Besides, a reasoned motion for conducting covert investigative actions is filed with a court by a prosecutor irrespective of whether this case falls within the jurisdiction of the State Inspector.[167] The above-mentioned hampers effective oversight and gives rise to misgivings regarding the impartiality of supervisory bodies.

The Constitutional Court observed in its judgment of 14 April 2016 that the effectiveness of the inspection can be guaranteed by "complete distancing of the inspector from the process."[168] However, vesting the State Inspector with investigative powers hampers the inspector's complete distancing from covert investigative actions.

The investigative department of the State Inspector's Service received 170 notifications in November 2019 and 181 notifications in December 2019.[169] Besides, considering the fact that the State Inspector is the safeguard for the protection of personal data, burdening the State Inspector's Service with such investigative powers casts doubts on whether it can carry out its statutory tasks adequately.

Interference with the right to respect for private life should be subject to effective, independent and impartial oversight.[170] Under the General Data Protection Regulation (GDPR), the competent authorities supervising the processing of personal data can be vested with investigative powers but only concerning an alleged infringement of the GDPR (e.g., whose data is being gathered and for what purposes).[171] For instance, in Lithuania, Latvia and Estonia, oversight bodies are vested with investigative powers only within the personal data protection field and they themselves do not carry out investigative powers usually falling within the mandate of law-enforcement authorities.

Stemming from all the above-mentioned, it is clear that vesting the State Inspector's Service with the investigative powers contradicts the best international practice, causes the ineffective discharge of tasks, increases the risk of infringement of the right to respect for private life and contributes to creating a conflict of interests among agencies.

[167] The Criminal Procedure Code, Article 143^3.1.

[168] See judgment of the first section of the Constitutional Court of Georgia, 1/1/625,640, adopted on 14 April 2016, para. 65.

[169] See the 2019 Report on the Activities of the State Inspector, p. 117.

[170] ECtHR, September 6, 1978, *Klass, v. Germany*, paras. 55 and 56.

[171] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

7. RECOMMENDATIONS

To the Parliament of Georgia

- To start discussions on the transfer of the power of inspection the legality of covert investigative actions and personal data processing to the independent state body, that in order to avoid a conflict of interests among agencies, will not be vested with investigative powers.
- To provide for the possibility of conducting covert investigative actions only concerning intentional crimes.

Concerning the LEPL Operative-Technical Agency

- To ensure full institutional independence of the LEPL Operative-Technical Agency;
- To restrict the Operative-Technical Agency in creating technical means of obtaining, possessing and administering personal information in real-time independently from service providers as well as its possibility of direct access to personal information through resorting to such means;
- To introduce statutory mechanisms that will exclude any possibility to create an alternative bank of data by the Operative-Technical Agency;
- To specify in the Law of Georgia on Electronic Communications the group of persons whose databases can be copied and retained by the Operative-Technical Agency; and
- To create statutory safeguards that would exclude the institution of covert investigative actions by the agency without notifying the State Inspector's Service; to determine appropriate responsibility for the failure to comply with the duty.

Concerning the Destruction of Material Obtained From Covert Investigative Actions

- To lay down a detailed procedure for the destruction of the material obtained from covert investigative actions;
- To specify in the legislation governing the operative and investigative activities the concrete procedures and the competent authority for the destruction of information obtained from covert investigative actions; and
- The material containing personal data obtained from covert investigative actions should be destroyed in the presence of the supervisory judge (if the case falls within the State Inspector) or a representative of the State Inspector's Service.

Concerning Judicial Control

- A prosecutor's motion for covert investigative actions should be examined only at an oral hearing;
- A judge with special training on the specific issue at stake should be authorised to adopt an order on covert investigative actions; and
- When issuing an order on covert investigative actions, a court should determine the date of notification of an object of covert investigative actions about the investigative action conducted against him/her; a prosecutor should retain the power of applying to the court after the elapse of this term regarding the extension of the term for no more than 12 months.

Concerning the State Inspector's Powers

- To specify in the legislation what type of infrastructure is accessible for the State Inspector's Service during the inspection of the Operative-Technical Agency and the inspection methods employed in this process;
- To determine by the legislation the mandatory minimum number of annual inspections of the Operative-Technical Agency to be carried out by the State Inspector; and
- To equip the State Inspector's Service with additional mechanisms of oversight along with inspection to control the agency's activities aimed at obtaining information from cyberspace.

To the State Inspector's Service

- To specify in the annual reports of the State Inspector's Service the methods employed during the inspection of the agency's activities, violations identified, the response/ recommendations of the State Inspector's Service and information about the fulfilment of recommendations by the Operative-Technical Agency.