The European Union for Georgia

NETHERLANDS HELSINKI COMMITTEE

IDFI
Institute for Development of Freedom of Information

OVERSIGHT OF COVERT SURVEILLANCE

LAW AND PRACTICE

2024

The preparation of this report was funded by the European Union. Its contents are the sole responsibility of the Institute for Development of Freedom of Information (IDFI) and do not necessarily reflect the views of the European Union.

CONTENTS

ABBREVIATIONS AND TERMINOLOGY

CPCG - Criminal Procedure Code of Georgia

CCG - Criminal Code of Georgia

Law on Agency - Law of Georgia “On the Legal Entity under Public Law – the Operative-Technical Agency of Georgia"

Law on Counter-Intelligence Activities - Law of Georgia “On Counter-Intelligence Activities”

Covert surveillance measures - covert investigative actions and electronic surveillance measures

Covert investigative actions - covert investigative actions provided for by Article $143^1(1)$(a-e) of the Criminal Procedure Code of Georgia

Electronic surveillance measures - Electronic surveillance measures provided for by Articles 9.2 (sub-paragraphs “a” and “b”) and 9.3 of the law of Georgia “On Counter-Intelligence Activities”

Rules of Procedure - Rules of Procedure of the Parliament of Georgia

Agency of SSSG - the Legal Entity of the State Security Service under Public Law – the Operative-Technical Agency of Georgia

SSSG - State Security Service of Georgia

IDFI - N(N)LE Institute for Development of Freedom of Information

Monitoring [reporting] Period - Period from January 1, 2021 to December 31, 2023

Venice Commission - European Commission for Democracy through Law

FINDINGS

1. There is not sufficient information to draw convincing conclusions about the compliance of the implementation of covert surveillance measures with human rights standards.

2. The quality of the statistical data processed by the responsible bodies regarding covert investigative actions is low. The statistical data provided by different institutions cannot be effectively compared or reconciled to draw meaningful conclusions.

3. Obtaining any information (including the most basic statistical data) regarding electronic surveillance carried out within the counter-intelligence activities is problematic, and there is no room for drawing any kind of substantive or quantitative conclusions regarding these covert surveillance measures.

4. It is impossible to assess the effectiveness and legality of judicial control over covert surveillance measures. Courts do not disclose the texts of relevant authorization orders, even after the criminal case is closed and the obtained information - destroyed.

5. Based on information obtained by IDFI, in 2021-2023, the common courts reviewed over 9300 motions regarding covert investigative actions. Almost 91.7% of them were granted either fully or partially.

6. Tbilisi City Court reviews the most motions, accounting for 54.7% of all motions reviewed by the courts.

7. Out of the courts, which considered more than 10 motions in the reporting period, three courts (Ambrolauri, Tsageri, and Akhalkalaki) granted 100% of the motions. Also, among large cities, the courts of Gori (99%), Mtskheta (98.3%), and Rustavi (96.5%) stand out with an exceptionally high rate of granting.

8. The number of cases where the prosecutor's office extended the notification period for individuals under covert surveillance increased by 80% after 2021.

9. There is no information regarding one of the covert investigative actions - “real-time geolocation identification”. It should be noted that the technical capabilities of real-time geolocation identification is a separate system that took significant resources of the state to build.

10. From March 1, 2022, to March 31, 2024, the Special Investigation Service initiated the investigation on 331 cases. As of March 31, 2024, the Special Investigation Service had 244 ongoing criminal cases under its competence. Criminal prosecution was initiated against 87 persons. None of these prosecuted individuals were officials responsible for carrying out covert investigative actions or representatives of special services that conduct electronic surveillance for counter-intelligence purposes.

11. In a number of cases, public institutions unlawfully reject applications requesting public information regarding covert surveillance. To obtain this information, an applicant is forced to make significant effort, including preparing applications and pursuing administrative complaints.

12. The Personal Data Protection Service did not/was not able to provide information on the period between 2021 to February 2022. The statistical data regarding covert investigative actions obtained from this agency is available only for the period after March 2022.

13. The constitutional control over covert surveillance is significantly limited. The cases under the review of the Constitutional Court of Georgia are unreasonably delayed.

STEPS TO BE TAKEN TO ADDRESS SOME OF THE CHALLENGES

1. Develop a methodology for processing statistical data regarding the covert investigative actions in coordination with the institutions involved in the supervision of this process, so that:

    1.1. Statistical information shall include data on various aspects of the covert investigative actions provided for by the Criminal Procedure Code of Georgia (for example: types of covert investigative actions, prolonging the covert investigative actions, results of appeals, postponement of notification, etc.);

    1.2. Information collected by different institutions on the same issues should allow comparison.

2. Process and publish statistical information regarding the covert surveillance measures conducted for counter-intelligence purposes;

3. Ensure that the judicial acts delivered on covert surveillance are public after the interest for its classification is extinguished;

4. Law enforcement agencies should have effective responses to cases of abuse of covert surveillance. Updated information about these responses should be proactively disclosed to the public.

5. Parliamentary control over the agencies responsible for the implementation and supervision of covert surveillance, as well as over the unlawful publication of covert materials, should be strengthened.

INTRODUCTION

The security and justice sectors are crucial for building a democratic and legal state. The accountability, impartiality, and adherence to the rule of law and human rights of these sectors are essential indicators of the quality of a country's democracy.

Unfortunately, in Georgia, there have always been legitimate concerns regarding the impartiality of the security and justice sectors, as well as their use for partisan interests. These concerns have even exacerbated in recent years. This is echoed by the European Commission's report of November 8, 2023 *(p. 33)*, which granted Georgia candidate status, however, challenges were identified in relation to almost every institution belonging to the justice or security sector. Among other things, this report mentioned the fact of September 13, 2021 - the massive leakage of materials, allegedly obtained and created as a result of unlawful covert surveillance. The European Commission indicated that, despite calls, the disclosure of information about the private lives of journalists, politicians, the diplomatic community, and civil activists has yet to be investigated. It is noteworthy that on December 18, 2023, the Venice Commission published its opinion, which, among other things, concerned the Personal Data Protection Service and the judicial control over the lawfulness of covert (investigative) actions *(par. 103-112)*. The Venice Commission once again voices concerns about the effectiveness of judicial control and considers the authority of the Personal Data Protection Service, to conduct technical monitoring on the Agency of SSSG, to be “uncommon” considering the nature of the service.

The likelihood of abusing the possibility of carrying out covert surveillance measures is particularly high, due to the covert nature of these actions as well as the the ease of achieving a legitimate or illegitimate goal. This is evident given the abundance of agencies and authorities aimed at preventing abuse of this authority of the state. The purpose of this analysis is to study these agencies and the usage of their authorities from the perspective of their transparency, accountability, and effectiveness.

THE SCOPE OF THE STUDY AND METHODOLOGY

IDFI primarily studied the national legislation regulating covert surveillance measures, as well as international and national standards of human rights protection. As a result, IDFI determined the standards of implementation of covert surveillance measures, their lawfulness, and compliance with the fundamental requirements of human rights protection. Regarding the implementation of these requirements in practice, IDFI studied the information available in open sources, after which the project team prepared public information requests.

IDFI addressed the Parliament of Georgia, the Agency of SSSG, the Personal Data Protection Service, the Special Investigation Service, the Prosecutor's Office, and the judiciary (the Supreme Court of Georgia, courts of appeals, and four city courts) with the applications requesting public information. The subject of the request was quantitative and substantive information regarding the covert surveillance carried out both for investigative and counter-intelligence purposes (including judicial acts) within the monitoring period (2021-2023 years). Furthermore, IDFI requested information on responses to the detected violations and publicly recorded incidents. Public information requests were formulated in such a way that the received information would be useful not only for quantitative but also for content/qualitative conclusions on covert surveillance in terms of pre-identified national and international standards. After analyzing the information received as a result of the first wave, IDFI sent additional public information requests as part of the second and third wave, furthermore, it filed administrative complaints to the relevant institutions.

For the interpretation of the legal norms, not only the views of the author were used, but also the explanations given by the relevant state institutions to the Constitutional Court of Georgia (minutes of the hearing) at the executive and substantive review sessions of the constitutional claims N885-1231.

For the purposes of this report, the covert surveillance measures under the SSSG Agency’s competence (besides the monitoring of postal and telegraphic transfer) were defined as the subject of the study. Namely, sub-paragraphs “a.a”-a.d” of Article 7 of the Law on Agency, as well as the sub-paragraph “a.f” of the same article. These measures are also defined by the sub-paragraphs “a”, “b”, “c” and “e” of paragraph 1 of the Article 143^1 of CPCG and the sub-paragraphs “a”, “b”, “d” of paragraph 2 of the Article 9, as well as the paragraph 3 of the same Article of the “Law on Counter-Intelligence Activities''.

1. NORMATIVE DEFINITION AND PRACTICAL UNDERSTANDING OF COVERT SURVEILLANCE MEASURES

According to the provisions outlined in subparagraphs “a.a”-”a.d” of Article 7 of the “Law on Agency”, as well as subparagraph “a.f” within the same Article, the Agency of SSSG is authorized to carry out the following actions for the purposes of achieving it designated objectives:

N1. a.a) covert eavesdropping and recording of telephone communication;

N2. a.b) obtaining information from a communications channel;

N3. a.c) obtaining information from a computer system;

N4. a.d) real-time geolocation determination;

N5. a.f) covert video and/or audio recording, photographing.

Article 143[1] of the Criminal Code of Georgia designates the aforementioned measures as covert investigative actions, while Article 9 of the Law on Counter-Intelligence Activities classifies them as operative-technical and electronic surveillance measures. It is important to note that the Agency has the exclusive authority to implement measures N1, N2, N3, and N4, and “the establishment and operation of another state body with similar functions and powers within the territory of Georgia is prohibited” *(Law on Agency, Article 12)*. As for measure N5, it may be carried out by both the Agency and other investigative bodies *(e.g., the Ministry of Internal Affairs, CPCG, Article 3.32.”b”)*.

It is important to note that, according to the legislation, the Agency does not make decisions itself regarding the application of these measures. Rather, the Agency should be viewed as a service provider body for the security and law enforcement sector, that is included in the governance sphere of the SSSG; however, according to the law, the Agency must be independent. Significantly, the lack of genuine independence of the Agency is one of the key arguments in the constitutional lawsuit initiated by the

Public Defender and 326 citizens, challenging the constitutionality of the SSSG's Agency's powers. The Constitutional Court has been considering these cases for the past seven years.

1.1. COVERT EAVESDROPPING AND RECORDING OF TELEPHONE COMMUNICATION

According to Paragraph 36 of Article 3 of CPCG, secret monitoring and recording of telephone communication means "the covert eavesdropping and recording of telephone communication performed through common usage electronic communication networks".

In practical terms, this refers only to **telephone communications** (GSM network), involving real-time wiretapping of the communication as they occur and recording of conversations for subsequent use. The scope of this covert measure does not include electronic communication, which is carried out not directly by telephone, but by using the internet network. For example, communications made through applications like "Messenger" are not considered as telephone communication.

1.2. OBTAINING INFORMATION FROM A COMMUNICATIONS CHANNEL AND A COMPUTER SYSTEM

Unlike the real-time eavesdropping and recording of telephone communication, obtaining information from a communication channel and/or computer system implies obtaining information already existing within these sources as well as information created in real time. In particular, the communication channel refers to a communication network, telecommunication, or information system from which the retrieval and recording of current, transmitted, received, collected, processed, or accumulated information is legally defined as a permissible investigative action *(CPCG Article 3.33)*. A similar action involves obtaining information from a computer system *(CPCG Article 3.34).* A computer system is defined

as any mechanism or a group of interconnected mechanisms that automatically processes data through software (including personal computer, any device with a microprocessor as well as mobile phones) *(CPCG Article 3.27).*

Obtaining information from a communication channel and computer system encompasses a wide range of information and various methods of obtaining it, from internet traffic data to video call recordings. This measure includes obtaining any data or information within the internet network as well as the sending or receiving device (photo, video, text, traffic information, etc.). To fulfill the task, the Agency is authorized to use all types of technical tools at its disposal, including so-called viruses (in normative language: "special software" *(Law on Agency, Article 2 "g")).* This measure is so diverse that some aspects are separated by legislation as a separate measure - for example, geolocation (location) data, which falls under communication channel information, is designated as a separate investigative action.

An example of obtaining information from a communication channel would be using a so-called computer virus to obtain messages or calls made through the "WhatsApp" application.

An example of obtaining information from a computer system would be acquiring a document saved on a personal computer.

1.3. REAL-TIME GEOLOCATION DETERMINATION

Real-time geolocation determination refers to determining the geographical location of a particular mobile communication device in real time, at the moment it is determined. This implies determining the geographical location with the highest possible accuracy *(CPCG Article 2.35).* As mentioned above, geolocation is the determination of the location of a communication device, such as a smartphone, within a specific timeframe, including in the current (live) mode.

A practical example of this measure is monitoring the movement of an object of interest to the state by tracking their smartphone.

1.4. COVERT VIDEO AND/OR AUDIO RECORDING, PHOTOGRAPHING

As for covert video recording, audio recording and/or photographing, it involves capturing the image, actions, communication with or without images of persons subject to this action, without their knowledge. This can take place in private spaces such as the subject’s residence, personal vehicle, or workspace. It should be noted that covert video and/or audio recording or photographing does not necessarily require a physical recording with a camera or photo camera. It can involve recording video and/or audio or taking photos by remotely accessing a person's computer systems (e.g., by remotely activating a laptop web camera or microphone). The technical tool of remotely accessing a person's computer systems for video/audio recording or photography was named as one of the forms of covert recording by the Agency's representative at the session of substantive consideration for lawsuits N885-1231 at the Constitutional Court of Georgia.

A classical example of covert video and audio recording involves placing hidden cameras and listening devices in living spaces.

2. TECHNICAL CAPABILITIES OF THE SSSG'S AGENCY TO CONDUCT COVERT SURVEILLANCE MEASURES

Conducting covert surveillance typically involves the use of sophisticated and complex technical methods, devices, and/or software. The state has always had the ability to carry out covert surveillance, but after 2014, the state's latitude, in terms of its technical capabilities, increased significantly. Specifically, the legal technical limitations on state-conducted covert surveillance have practically equated with overall technological advancements. This was a result of allowing the state, specifically, the SSSG's Agency to directly access the infrastructure of telecommunications service providers, including their communications networks.

According to the current framework, every authorized electronic communications provider company in Georgia has an obligation to allow the Agency to access its infrastructure, resulting in the ability of the Agency to install devices and software on it in order to achieve the goals set by the law. For example, obtaining the content and identification data of telephone and internet communications, real-time geolocation identification; creation of a unified system of identification data of electronic communications - so-called "identification central bank", etc.

The legislation tries to create safeguards for the threats coming from direct technical access not only through classical procedural safeguards, protecting the right to private life (preliminary or post-factum judicial authorization), but also, by introducing the mechanisms of technical control. For example, a special electronic control system, which, in most of cases, allows the Personal Data Protection Service and the Supreme Court of Georgia to exert technical control over the activities of the Agency. Naturally, according to the Criminal Code of Georgia, unlawful application of this technical ability, as well as, concealment of such information is a crime. And, if the state authorities do not properly exercise their function, the Parliament of Georgia is entitled to use its control powers (for example, investigation commission, impeachment, etc.). It is noteworthy that the direct access of the SSSG's Agency to telecommunications network

infrastructure, as well as the threats stemming from it, became the main reason for declaring unconstitutional Agency's this capability. The norms that replaced the unconstitutionally recognized norms were once again subject to a constitutional lawsuit before the Constitutional Court of Georgia since the Public Defender and the civil society organizations considered the new norms as pseudo changes. The Constitutional Court is considering these lawsuits for the 7th year already.

This report will step-by-step review the legal procedure established by the legislation of Georgia and based on the legislation and the information/data obtained by IDFI will assess the degree of transparency, accountability, and effectiveness of the bodies responsible for the prevention of abuse/illegal use of the technical capabilities at disposal of the SSSG's Agency.

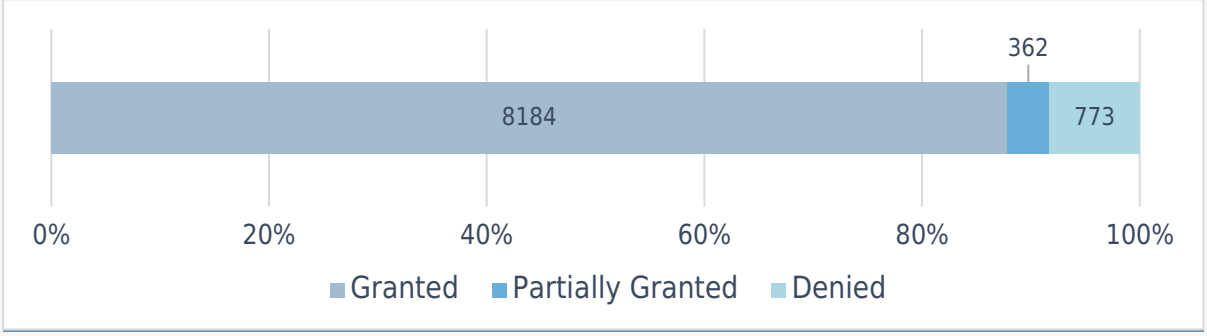
3. OBJECTIVES, LEGAL BASIS, AND PRACTICE OF COVERT SURVEILLANCE

The legal procedural framework for executing covert surveillance measures does not differentiate among the various types of them. An identical legal regime is applicable for each kind of surveillance measure. Since covert surveillance is a source for acquiring critical information, it poses a significant risk of unduly infringing upon fundamental rights and freedoms. Therefore, essential preconditions must be satisfied for its implementation to be justified and lawful.

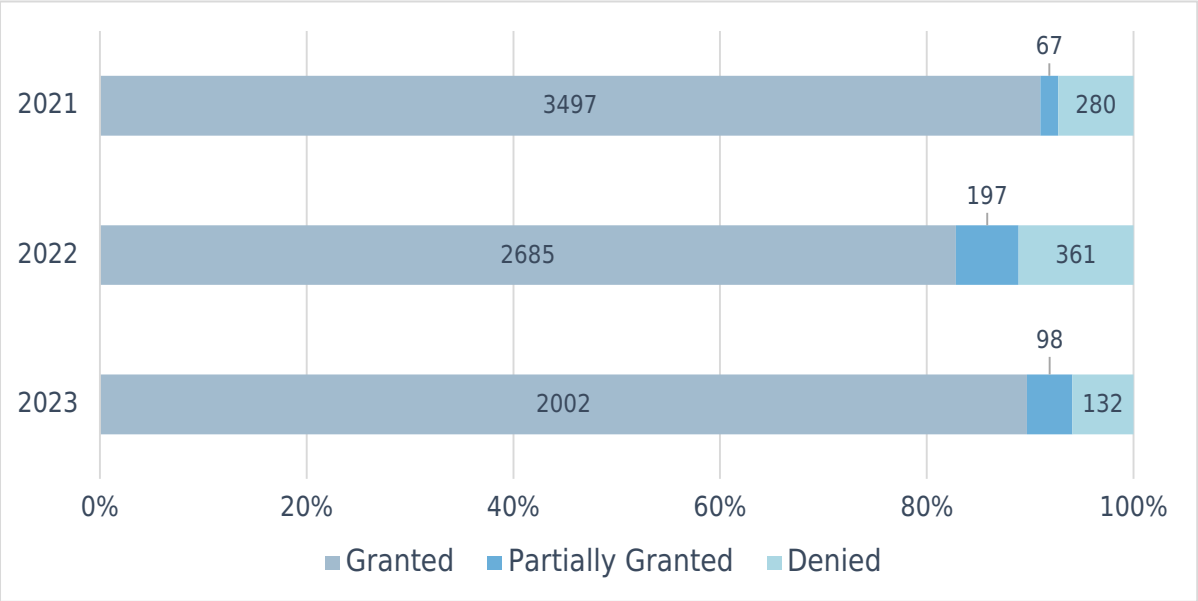
Taking into account the specific focus and objectives of this report, the implementation of covert surveillance measures for investigative purposes on the one hand, and counterintelligence activities on the other hand, will be reviewed separately.

3.1. IMPLEMENTATION OF COVERT SURVEILLANCE MEASURES DURING THE INVESTIGATION PROCESS

According to the legislation of Georgia, the Supreme Court is responsible for the collection and publication of information on covert investigative actions. The data provided by the Supreme Court of Georgia indicates that during the period covered by the report, more than 9,300 motions for covert investigative actions were reviewed and almost 91.7% of them were fully or partially granted.



It is important to note that the information provided by the Supreme Court covers all types of covert investigative actions and is not limited to those identified in the research methodology. The monitoring period, depending on the years covered, looks as follows:



For the purposes of the Criminal Procedure Code, the Prosecutor's Office of Georgia has the authority to apply to the court for conducting a covert investigative measure. Initially, the FOI request of IDFI addressed to the General Prosecutor's Office of Georgia was left unanswered. Only after an administrative complaint that was partially granted, the requested statistical data was provided to IDFI incompletely.

The provided information indicates that during the monitoring period, the Prosecutor's Office executed only three of the six covert investigative actions listed in the first paragraph of Article 143[1] of CPCG. In particular, the Prosecutor's Office did not employ the following covert surveillance measures:

- Real-time geolocation identification;
- Monitoring of a postal and telegraphic transfer (except for diplomatic mail);
- Electronic surveillance through technical means.

3.1.1. AUTHORIZATION FOR COVERT INVESTIGATIVE ACTIONS

A decision to conduct covert investigative actions is made and authorized by the district (city) court based on a reasoned motion of a prosecutor *(CPCG, Article 143³.1)*. However, when "a delay may cause destruction of the facts important to the case (investigation), or make it impossible to obtain those data", the prosecutor has the authority to conduct/initiate covert investigative action by her/his own resolution *(CPCG, Article 143³.6)*. The measures conducted/ongoing on the basis of the prosecutor's request are temporary and can be authorized for a maximum of 48 hours. Within this period, the prosecutor must address the relevant district (city) court in 24 hours. Then the court makes a final decision regarding the lawfulness of the conducted/ongoing covert surveillance measure within 24 hours of receiving the motion (SCC, *CPCG, Article 143³.6*).

The judge's ruling on the execution of covert investigative action must be documented in four copies. One copy is retained by the court, two copies are provided to the requesting prosecutor or a representative of an investigative body, and a final copy, containing only the relevant requisites and the resolution, is forwarded to the Personal Data Protection Service. One of the two copies given to the prosecutor or the representative of the investigative body must be delivered to the Agency in material form immediately after its issuance, but no later than 48 hours *(CPCG, Article 143³.5)*.

The data provided by the Prosecutor's Office of Georgia indicates that during the monitoring period, the city (district) courts received the following number of motions from the Prosecutor's Office requesting the implementation of these covert investigative actions:

TYPE OF THE COVERT INVESTIGATIVE ACTION	2021	2022	2023
Covert eavesdropping and recording of telephone communication	1398	1546	1067
Covert video and/or audio recording, photographing	861	1191	1097
Obtaining information from a communications channel and a computer system	8	1	3
Total	2267	2738	2167

The only exception to this general rule is the case when the target of the covert investigative action is a state political official, a judge or a person having immunity. In such cases, the implementation of the measure must be authorized by a ruling from a Supreme Court judge, which is granted based on a reasoned motion from the General Prosecutor or her/his deputy *(CPCG, Article 143³.17)*. During the reporting period, the General Prosecutor/Deputy exercised this authority eight times to conduct two types of covert investigative actions:

COVERT INVESTIGATIVE ACTIONS TARGETING INDIVIDUALS HOLDING HIGH POLITICAL AND STATE POSITIONS / ENJOYING PRIVILEGES OF LEGAL IMMUNITY	2021	2022	2023
Covert eavesdropping and recording of telephone communication	3	1	0
Covert video and/or audio recording, photographing	3	1	0

As for the covert investigative action carried out/initiated based on the prosecutor's resolution due to urgent necessity, the provision of the judge's ruling regarding its recognition as legal or illegal to the relevant agencies is regulated in the same manner as described in the previous case of measures conducted based on the judge's ruling *(CPCG, Article 143³.7)*.

While the data provided by the Prosecutor's Office following the administrative complaint partially addressed the IDFI's request for public information, a significant part of the requested data, which would be crucial for evaluating the effectiveness and legality of the implementation of covert investigative actions in various aspects, remained unaddressed. For instance, the Prosecutor's Office response did not reveal information about the types of motions (whether for prior approval or for the legalization of actions taken due to urgent necessity), the approval rate of motions, the duration of each investigative action, and the relevant articles of the Criminal Code (crimes) to which the covert investigations were conducted.

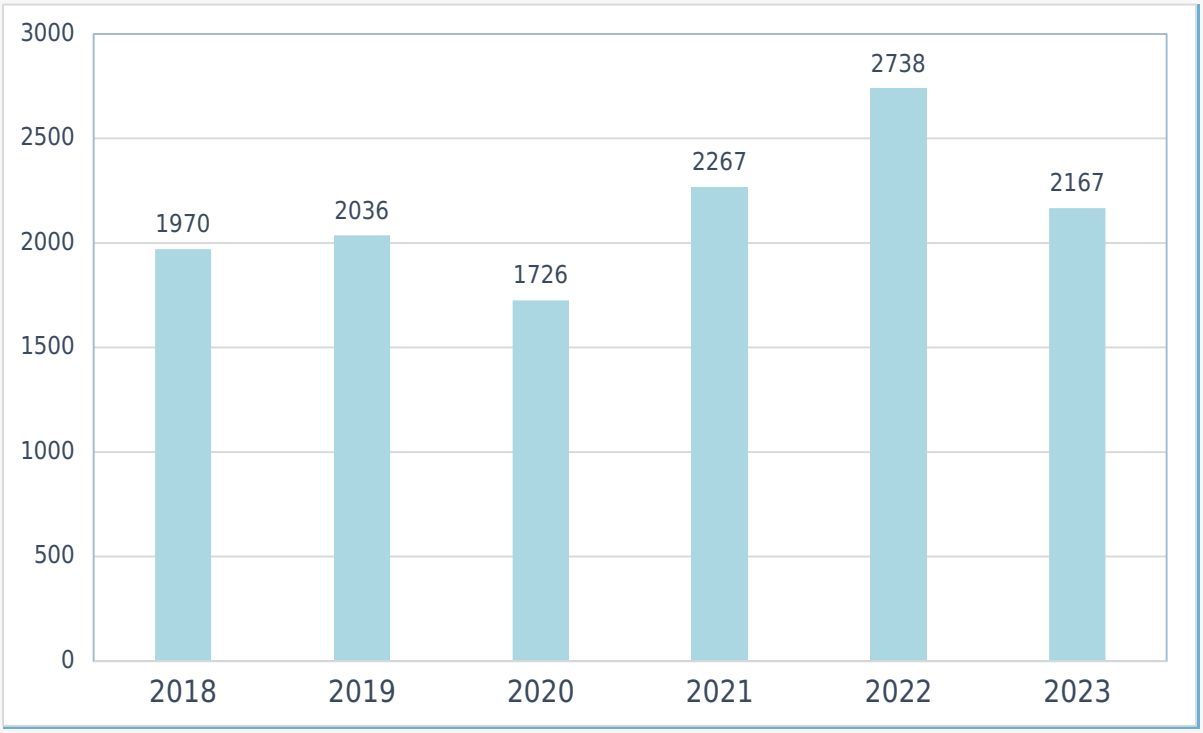
Nevertheless, since IDFI requested this data from various agencies, it is possible to draw some general conclusions. In particular, law enforcement agencies under the investigative supervision of the Prosecutor's Office frequently require court authorization and the technical capabilities of the Agency of SSSG. The public information obtained from these two institutions provides the opportunity to indirectly fill in the missing data received from the Prosecutor's Office.

The data provided by the Agency of SSSG suggests that during the monitoring period, the percentage of covert investigative actions conducted due to urgent necessity is decreasing (2021 9%, 2022 6%, 2023 3%):

TYPE OF THE COVERT INVESTIGATIVE ACTION	2021	2022	2023
Covert eavesdropping and recording of telephone communication	1334	1380	998
	92	65	16
Covert video and/or audio recording, photographing	741	918	901
	98	72	37
Obtaining information from a communications channel and a computer system	7	2	1
	0	0	0

- **Authorization of court** - **Urgent Necessity**

Overall, the analysis of the statistical information provided by the Prosecutor's Office in the dynamics of previous years reveals a fluctuating yet increasing trend. (2018-2020 summary data for identical covert investigative actions are taken from IDFI's 2021 report):

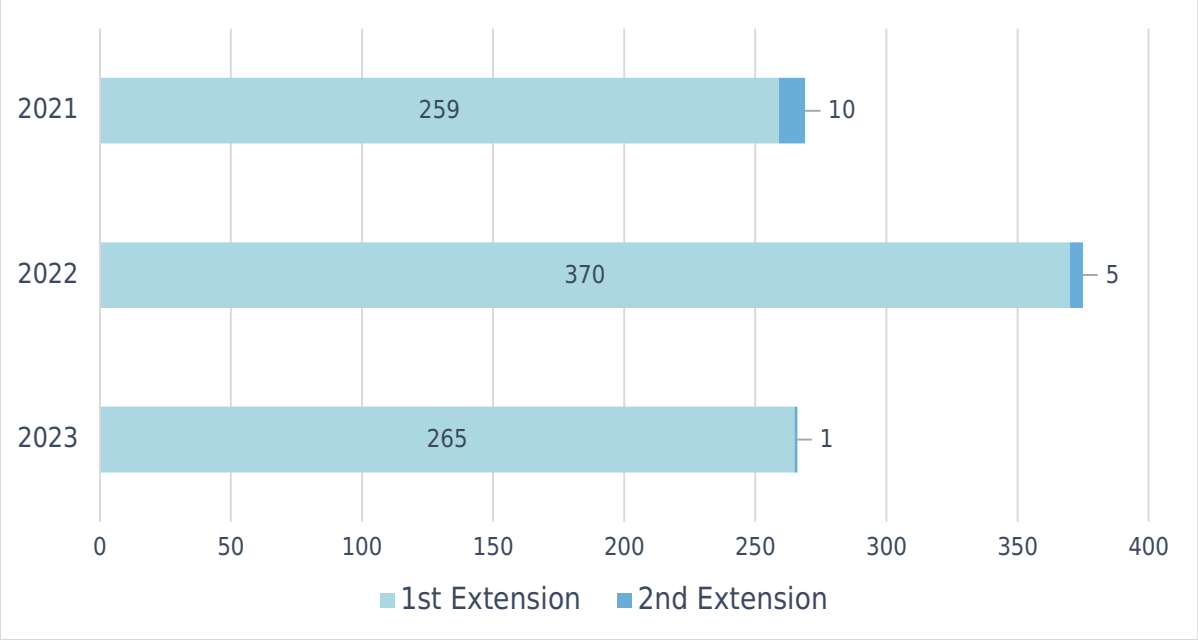


3.1.2. TIME LIMITS FOR THE IMPLEMENTATION OF COVERT INVESTIGATIVE ACTIONS

A judge's ruling on the implementation of covert investigative action, as well as on the lawfulness of using it in case of urgent necessity, must include such necessary elements that are of critical importance for the lawful implementation and oversight of the measure. Specifically, alongside the typical requirements of a legal document (such as the name of the prosecutor who submitted the request, the criminal case number, etc.), the ruling should specify the timeframe authorized by the judge for implementing the measure, including its start and end date and time limits *(CPCG, Article 143[3].10).*

In general, covert investigative actions are carried out in three stages, with a maximum period of 90 days for each stage. A judge's approval for progressing through each phase is determined by motions from prosecutors at various hierarchical levels of the prosecution system. In particular, the first stage is carried out by a motion of a prosecutor, the judge authorizes the transition to the second stage based on the request of a senior prosecutor, and the third stage requires a motion from the General Prosecutor or her/his deputy. In addition, while the 90-day period is the maximum allowed, the judge may authorize a shorter duration. If the objectives of the relevant investigation have not been achieved, the requesting prosecutor/senior prosecutor/general prosecutor or her/his deputy may request its extension. Progression to each subsequent stage of implementation of covert investigative measures is allowed only if the objectives of this action have not been met in the current stage. There is an exception to this general rule, which allows for a covert investigative action to continue for an additional 90-day periods unless the objective of the action is not achieved. This exception applies to ongoing investigations into crimes specified in the Criminal Code and is permitted only upon the motion of the General Prosecutor or her/his deputy. On a similar basis, the above-mentioned 3-stage system can be extended once for another 90 days in the case provided by the law of Georgia "On International Cooperation in Criminal Matters" *(CPCG, Article 143[3].11-12[7])*.

The data provided by the Prosecutor's Office of Georgia indicates that in the monitoring period, the rule of one-time extension was applied. The extension was only used in relation to covert investigative actions such as telephone and video/audio recording as well as photography. Specifically, covert telephone surveillance was extended in 68% of cases, while covert audio/video recording and photography were extended in 32% of cases.



It is important to note that the data for 2022 and 2023 in this chart does not align with the information provided by the Personal Data Protection Service. In particular, according to the Service, in 2023, there were 350 requests for extensions of investigative actions, whereas in 2022, there were 474 requests within a ten-month period. The reason for this discrepancy is unclear, particularly given that acts of electronic surveillance for counter-intelligence purposes are not submitted to the Personal Data Protection Service. Additionally, the authority to request extensions for investigative actions in all other instances lies solely with the court, with only the prosecutor able to make such requests (see Subchapter 5.1).

3.1.3. TERMINATION OF A COVERT INVESTIGATIVE ACTION

Regarding the termination of a covert investigative action before the expiration of the period specified for it, the decision is made by the prosecutor on the basis of an investigator's appeal, or on her/his own initiative. The prosecutor must immediately inform the state body or agency that practically implements the action. This decision may be based on various circumstances such as the achievement of investigation objectives; circumstances are discovered that confirm that the specific

objective provided for by the ruling on the given covert investigative action cannot be achieved due to objective reasons, or the carrying out of the covert investigative action is no longer essential to the investigation; termination of the investigation or prosecution itself; changing the legal basis for its implementation; in cases where the event has been suspended, the removal of the reasons for suspension within three days. Additionally, covert investigative action that was initiated due to urgent necessity can be terminated by a judge's ruling if the prosecutor's resolution is declared illegal *(CPCG, Article 143[6] 1-4).*

TERMINATION OF THE COVERT INVESTIGATIVE ACTION	2021	2022	2023
Covert eavesdropping and recording of telephone communication	84	109	103
Covert video and/or audio recording, photographing	113	162	197

3.1.4. DESTRUCTION OF INFORMATION OBTAINED FROM COVERT INVESTIGATIVE ACTIONS

Due to the extremely sensitive nature of the information obtained as a result of covert investigative action, legislation emphasizes the need to store this information only when absolutely necessary and outlines the conditions under which it should be destroyed. The authority responsible for destroying this information is governed by regulations, which are related to the basis of the destruction of information itself.

Namely, the obtained information must be destroyed upon the termination or completion of the action if it is determined that it has no value for the investigation. Similarly, information obtained through the investigative action authorized by a judge as an urgent necessity must be destroyed if it is not presented to the court during the criminal case proceedings on merits. In addition to the afore-mentioned occasions, the information

obtained through the operative-investigative activities, which does not contain data related to criminal activity, but reveals personal details about individuals, must also be destroyed *(CPCG, Article 143[8].5).*

In each of these circumstances, the decision to destroy the information is made by the prosecutor in the presence of a judge/a judge of the court who/whose judge made a decision on the carrying out of this covert investigative action or recognized as lawful/unlawful the covert investigative action carried out without a court ruling in the case of urgent necessity *(CPCG, Article 143[8].5).*

	2021	2022	2023
Destruction of the information gathered through covert investigative actions by years	19	8	2

Regarding other grounds for the destruction of obtained information, the legislation outlines two specific occasions - the first involves information that was presented in court but deemed inadmissible by the judge, while the second one refers to the information, which is attached to the case as material evidence.

Inadmissible information obtained as a result of a covert investigative action must be destroyed immediately 6 months after the final judgment by the court of the last instance in the case. Information attached to the case in the form of material evidence must be retained for the entire duration of the criminal case and then destroyed without delay afterward. In both cases, the authority and responsibility for the destruction of this information lies with the judge who authorized the investigative action or recognized the action initiated by urgent necessity as lawful *(CPCG, Article 143[8].2,3,6*).

According to the data provided by the Supreme Court of Georgia, there were 19 cases of destruction of material obtained as a result

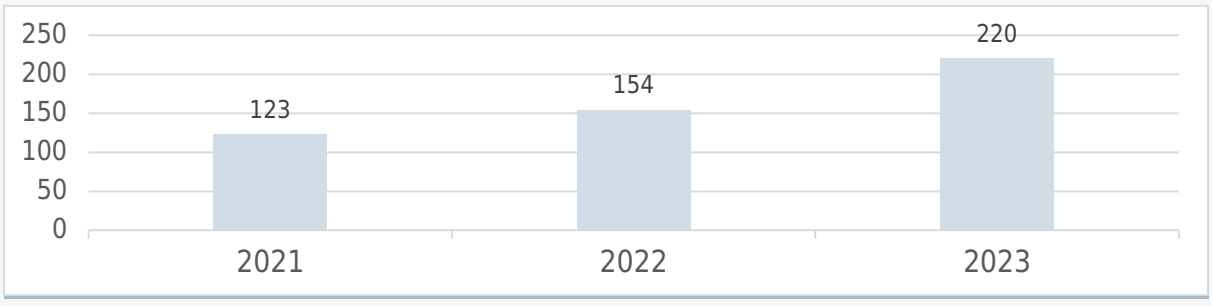
of covert investigative action by common courts, with 17 occurring in Tbilisi and 2 in Kutaisi.

3.1.5. NOTIFICATION TO A TARGET PERSON ABOUT THE COVERT INVESTIGATIVE ACTION TAKEN

The target of the covert investigative action is not informed about the ongoing action during its implementation. This is possible only upon its completion *(CPCG, Article 143[9].1)*. Additionally, one occasion for such notification is the exchange of evidence/information between parties five days before the pre-trial sitting on a criminal case, as well as during the signing of a plea bargain *(CPCG, Article 83.6)*.

In all other cases, whether during the criminal case or after its conclusion, the prosecutor decides when to inform the target about the covert actions, the content of the information acquired, or its destruction. If a decision on notification is not made by the prosecutor within 12 months after the end of the case, the prosecutor must seek permission to delay the notification for no longer than another 12 months from the judge or court that authorized the covert investigative action *(CPCG, Article 143[9].3,4)*. The prosecutor may request a 12-month extension of the notification two more times. Additionally, in relation to specific crimes, there is no restriction on making such a request, and notification to a person can be postponed until the expiration of the statute of limitations *(CPCG, Article 143[9].5,6)*.

The number of motions by the Prosecutor's Office to extend the notification period for covert investigative actions is increasing significantly:



In terms of the notification of covert investigative actions, it is worth noting that according to CPCG, the targeted person is granted the opportunity to file an appeal with the investigative panel of the Court of Appeal. This can be done during the pending proceedings or following their completion as well. If the appeal is successful, the evidence obtained through the unlawful action might be ruled inadmissible. Furthermore, it may provide grounds for the revision of a judgment, provided the evidence obtained as a result of that covert investigative action served as grounds for that judgment. In either case, the subject of the action can seek compensation for damages resulting from the violation of her/his right to privacy *(143[3].14,15)*.

3.1.6. QUANTITATIVE OBSERVATIONS ON COVERT INVESTIGATIVE ACTIONS

The presented statistical information raises numerous questions in terms of its quality and reliability. Data from different agencies cannot be compared, and there are discrepancies that can only be explained by vague assumptions. Despite this, a few observations can still be made.

Despite the fact that in 2022 the Parliament of Georgia significantly expanded the list of crimes for which covert investigative actions can be conducted, the statistical data of covert investigative actions has not changed significantly. However, there is a significant increase in the rates of deferring/extending notification to a person about covert actions. Against this background, it is unclear what the real purpose of the changes was, which earned local and international criticism.

A quantitative analysis of covert investigative actions indicates that the Tbilisi City Court considers the highest number of motions on covert surveillance, accounting for 54.7% of the motions considered by the courts.

COURT	CONSIDERED	GRANTED	PARTIALLY GRANTED	DENIED	% GRANTED
Tbilisi	5101	4431	274	396	92.24%
Rustavi	797	755	14	28	96.49%
Zugdidi	760	593	39	128	83.16%
Gori	670	661	2	7	98.96%
Kutaisi	458	410	8	40	91.27%
Batumi	403	365	3	35	91.32%
Mtskheta	176	170	3	3	98.30%
Telavi	173	135	1	37	78.61%
Bolnisi	136	118	2	16	88.24%
Akhaltsikhe	77	74	1	2	97.40%

Among the courts that considered more than 10 motions for covert investigative actions per year, the courts of Ambrolauri, Tsageri, and Akhalkalaki stand out with the highest approval rate (100% fully approved). Gori also stands out with 99%.

COURT	CONSIDERED	GRANTED	PARTIALLY GRANTED	% GRANTED
Ambrolauri	37	37		100.00%
Tsageri	31	31		100.00%
Akhalkalaki	28	28		100.00%
Gori	670	661	2	98.96%
Khashuri	66	65		98.48%

Mtskheta	176	170	3	98.30%
Sighnaghi	55	54		98.18%
Akhaltsikhe	77	74	1	97.40%
Rustavi	797	755	14	96.49%
Ozurgeti	55	52	1	96.36%

An interesting observation can be made regarding the percentage of eavesdropping in covert investigative actions. Specifically, in courts where the number of motions considered for eavesdropping exceeds 100, the percentage of these motions involving eavesdropping varies significantly (from 15% to 50%). For example, in Tbilisi, this rate is 43%, while in Rustavi, it is 15%.

The analysis of motions reviewed for covert eavesdropping in relation to crimes provided for in the Criminal Code indicates that covert eavesdropping is most often carried out within the framework of investigating the following crimes:

COVERT EAVESDROPPING AND RECORDING BY CRIME	CONSIDERED	GRANTED	% GRANTED
Membership of the Criminal underworld (“Being a Thief in Law”)	653	602	92.19%
Fraud	391	354	90.54%
Drugs-related crime	247	220	89.07%
Damage of Health	205	150	73.17%
Murder	189	161	85.19%
Theft	172	112	65.12%
Extortion	122	110	90.16%

Credit fraud	111	76	68.47%
Bribe	102	100	98.04%
Money Laundering	101	99	98.02%

3.2. COVERT ELECTRONIC SURVEILLANCE WITHIN THE FRAMEWORK OF COUNTER-INTELLIGENCE ACTIVITIES

When discussing individual counter-intelligence measures, it should first be noted that, for the purposes of this report, IDFI's research and analysis focus on assessing the transparency of covert surveillance measures conducted within the territory of Georgia. Therefore, this report does not cover strategic and individual monitoring measures that relate to electronic communications outside the territory of Georgia, as well as in territories where Georgian jurisdiction does not extend *(Law on the Agency, Article 2. "a". "b").*

The primary distinction between covert surveillance measures carried out for criminal and counter-intelligence purposes lies in the objective of such measures. While investigations aim to gather information directly relevant and essential to the investigation of a crime, the goal of counter-intelligence activities is to obtain information that ultimately poses a threat to national security interests, whether it be a person's connection to terrorist activities or the preparation/commission of actions directed against the national security interests of Georgia *(Law on Counter-intelligence activities, Article 10).* It is precisely for these purposes that measures carried out within the framework of counter-intelligence activities, including electronic surveillance measures, have the objective of obtaining information about intelligence or terrorist activities; or "to identify and prevent intelligence or terrorist acts and the circumstances related to their commission" *(Law on Counter-intelligence activities, Article 3)*.

3.2.1. LEGAL GROUNDS FOR CONDUCTING COVERT ELECTRONIC SURVEILLANCE MEASURES

Electronic surveillance may be conducted when there is data on facts or phenomena (or their signs) that pose or potentially may pose a threat to the state security of Georgia; as well as data on representatives or representation offices of foreign countries, which are related to intelligence and/or terrorist activities and the preparation or implementation of acts directed against the interests of the state security of Georgia or the grounds for such assumption; or data on Georgian persons, indicating their relation to the intelligence and/or terrorist activities of special services of foreign states *(Law on Counter-intelligence Activities, Article 10)*.

3.2.2. AUTHORIZATION OF COVERT ELECTRONIC SURVEILLANCE MEASURES

Similar to covert investigative actions, electronic surveillance can only be carried out pursuant to a court order or, in urgent cases, based on a decision by an authorized person subject to subsequent judicial review *(Articles 13 and 14 of the Law on Counter-Intelligence Activities)*. In such cases, the time limits specified in the above chapter apply to the issuance of this authorization, but the circle of authorized persons differs.

Specifically, the authority to issue orders for electronic surveillance, as well as the power to determine the legality of electronic surveillance conducted in urgent necessity cases, lies not with a city (district) court, but with a Supreme Court judge designated by the Chairperson of the Supreme Court of Georgia (supervising judge), as stipulated in Articles 2(u), 13.1, and 14.2 of the Law on Counter-Intelligence activities.

The entities initiating electronic surveillance measures also differ. Specifically, this authority is vested in certain departments of the State Security Service and the Ministry of Internal Affairs of Georgia (as defined in the list of special services for the purposes of subparagraph “t” of Article 2 of the Law of Georgia “On Counter-intelligence Activities,” as approved

by Government Resolution No. 448 of October 5, 2017, paragraphs 1 and 2; these departments are: General Inspectorate (Department); Counter-intelligence Department; Anti-Corruption Agency (Department); Counter-terrorism Center (Department); State Security Department; and v) Security Protection Regime Department; and, within the Ministry of Internal Affairs of Georgia: General Inspectorate (Department); Strategic Pipelines Protection Department; and the Border Police of Georgia), which are referred to as "special services" *(Article 2(t) of the Law on Counter-Intelligence activities)* and which have the authority to apply to the Supreme Court for the authorization of electronic surveillance measures or, in urgent necessity cases, to initiate such measures by their own decision *(Article 12, 14.1 of the Law on Counter-Intelligence activities).* It should be noted that the law stipulates identical timeframes for both the issuance of orders and the judicial review of measures initiated in urgent necessity cases, as for the covert investigative actions (see subsection 3.1.1 of this report) *(Article 13.2, 14.1 of the Law on Counter-Intelligence activities).*

3.2.3. GUIDING PRINCIPLE FOR AUTHORIZING COVERT ELECTRONIC SURVEILLANCE MEASURES

Similar to covert investigative actions, it is essential that measures carried out within the framework of counter-intelligence activities comply with the principles that court decisions must adhere to.

First and foremost, the decision must substantiate the existence of circumstances that could justify electronic surveillance. Moreover, such surveillance may only be used when it is necessary to achieve a legitimate aim in a democratic society and must be a proportionate measure. In the context of counter-intelligence activities, such a legitimate aim may only be national security. In addition to the aim, a decision to use electronic surveillance in counter-intelligence activities must also justify that the counter-intelligence information cannot be obtained by other means. This latter requirement imposes a stricter standard than that for covert

investigative actions, where it may also be justified that, theoretically, information could be obtained by other means, although this would require an unreasonably large effort *(Article 12.2 of the Counter-Intelligence Law).*

Additionally, in cases of electronic surveillance initiated in urgent necessity, the motion to the court by an authorized representative of the special service must include a justification for such urgency *(Article 14.1 of the Counter-Intelligence Law)*.

3.2.4. TIMELINES OF COVERT ELECTRONIC SURVEILLANCE MEASURES

Regarding the duration of electronic surveillance measures carried out within the framework of counter-intelligence activities, the three-stage extension system discussed in the previous chapter does not apply. The primary requirement is to conduct such a measure for the minimum period necessary to achieve the relevant goals; however, this period shall not exceed 90 days. This period may be extended by a supervising judge's decision as many times as the fulfillment of the measure's goals requires, but each time for a maximum period of 12 months *(Counter-intelligence Law, Article 13.4, 5)*. The judge's decision is based on a motivated motion by the special service, and the decision made by the judge must reflect the justification necessary for issuing the initial order *(Counter-intelligence Law, Article 13.5).*

3.2.5. TERMINATION OF THE COVERT ELECTRONIC SURVEILLANCE

Similar to covert investigative actions, there are circumstances under which an initiated measure must be terminated. Naturally, when a judge's order specifies a certain time limit, the expiration of that time limit constitutes one such termination circumstance. However, this is not the only ground. The measure must also be terminated when it was initiated due to urgent necessity, but subsequently, the supervising judge did not recognize this

necessity as lawful. In this case, as well, the measure must be terminated immediately *(Counter-intelligence Law, Article 14.2, 14⁴.1.g).*

Furthermore, electronic surveillance measures must be terminated when the task of electronic surveillance specified in the supervising judge's order has been completed *(Law on Counter-Intelligence Activities, Article 14⁴.1.a).* In this case, the decision to terminate is made by the head of the special service *(Counter-intelligence Law, Article 14⁴.2)*. Early termination of the measure may also be allowed when it is determined that the obtained information no longer has significant value for counter-intelligence purposes, or that achieving the specified goal is objectively impossible *(Counter-intelligence Law, Article 14⁴.1.b)*. In this case, the decision to terminate may be made by either the head of the special service or the supervising judge *(Law on Counter-Intelligence Activities, Article 14⁴.3).*

3.2.6. DESTRUCTION OF THE INFORMATION OBTAINED THROUGH COVERT ELECTRONIC SURVEILLANCE

Concurrent with the termination of electronic surveillance measures, the issue of destroying the information obtained as a result of such measures arises.

As a general rule, information obtained as a result of electronic surveillance that does not have value for the purposes of these measures shall be destroyed by the head of the special service in the presence of a supervising judge. This rule applies if the obtained information is not transferred to the relevant investigative body *(Law on Counter-Intelligence Activities, Article 14⁹.1).*

Furthermore, information obtained as a result of a measure initiated due to urgent necessity shall be immediately destroyed if the supervising judge does not recognize this measure as lawful *(Law on Counter-Intelligence Activities, Article 14.2).*

3.2.7. NOTIFICATION OF THE TARGET ABOUT THE IMPLEMENTED COVERT ELECTRONIC SURVEILLANCE MEASURES

It is mandatory to notify a targeted person about the implemented electronic surveillance measures, upon completing such measures. However, this obligation only exists after the notification itself will no longer harm the purpose of the measure. Moreover, it is considered unacceptable to provide notification in a situation where the disclosure of relevant information and documentation may endanger national security or democratic order; also, when the disclosure of information and methods of obtaining information endangers the tasks of counter-intelligence activity itself *(Law on Counter-Intelligence activities, Article 14^{10}.1,2).*

The decision to notify a person is made by the head of the special service *(Law on Counter-Intelligence Activities, Article 14^{10}.3).* Interestingly, while the prosecutor decides on notifying a person about covert investigative action, the latter is still obliged to apply to the court if no decision is made on notification within 12 months. The prosecutor needs the court's permission to extend this 12-month period. However, such judicial control is completely absent in relation to notification about the electronic surveillance measures conducted for counter-intelligence purposes. Accordingly, in this case, notifying a person is entirely dependent on the head of the special service.

3.2.8. ACCESSIBILITY OF STATISTICAL DATA ON ELECTRONIC SURVEILLANCE MEASURES CARRIED OUT FOR COUNTER-INTELLIGENCE PURPOSES

Within the framework of the project, IDFI, through public information requests, requested statistical data on the implementation of electronic surveillance provided for by the Law of Georgia "On Counter-intelligence Activities" in 2021, 2022, and 2023. The applications were addressed to the SSSG's Agency and the Supreme Court of Georgia. Based on responses to

public information requests, the project team aimed to assess how realistic it is to draw convincing conclusions about the lawful application of these measures.

To obtain statistical data on electronic surveillance measures, IDFI applied to the Operational-Technical Agency. One part of the public information request concerned data on covert investigative actions *(in detail, see chapter 3.1.1),* while the other part concerned electronic surveillance measures carried out for counter-intelligence purposes. Specifically, it was requested to provide the number of orders issued by the supervising judges of the Supreme Court to the agency regarding the conduct of these measures, both as prior authorization orders and in urgent necessity cases (separately, for each type of electronic surveillance, years, and special services).

The Agency provided IDFI with information only about covert investigative actions, while **the request related to the electronic surveillance measures conducted for counter-intelligence purposes was left unanswered.**

IDFI also attempted to obtain this data from the Supreme Court of Georgia. Specifically, it requested statistics on motions submitted to the supervising judge of the Supreme Court, their granting rate, as well as statistics on the use of the mechanism for suspending/terminating these measures, and the names and surnames of the judges who perform the function of "supervising judge". The Supreme Court did not provide IDFI with this information, after which IDFI filed an administrative complaint with the court. The Supreme Court's manager's decision (decision No. Z-251-24 of June 26, 2024) did not grant the complaint (in the part concerning electronic surveillance measures carried out for counter-intelligence purposes). **The Supreme Court considered any information related to electronic surveillance, including statistical data and the identity of the supervising judge(s), to be a state secret.**

It should be noted that **the court broadly applies the regime of state secrets to any information (including statistical) related to counter-intelligence activities, in violation of the rules provided by the Law of Georgia "On State Secrets."** The Supreme Court has not presented any specific legal basis, classification marking, or other document confirming that the information requested by IDFI was classified in accordance with the law.

Attempts to obtain public information have shown that obtaining any information related to electronic surveillance (including the most basic statistical data) is problematic. There is no room for drawing any kind of substantive or quantitative conclusions regarding covert surveillance measures conducted within the framework of counter-intelligence activities.

4. EVALUATION OF THE TRANSPARENCY, ACCOUNTABILITY, AND EFFECTIVENESS OF THE JUDICIAL OVERSIGHT OVER THE COVERT SURVEILLANCE

As part of the project, the second category of requested public information included judicial acts related to the judicial control of covert surveillance measures - rulings on covert investigative actions and orders for electronic surveillance as outlined in the Law of Georgia "On Counter-Intelligence Activities."

IDFI aimed to evaluate the accessibility of judicial acts related to covert surveillance and examine on what level are the legal standards and human rights protection requirements, as well as standards of proof, applied in decisions on authorization/lawfulness or illegality of covert surveillance measures by the courts, accessible and transparent to the general public, and, in general, how the effectiveness of judicial control is ensured. Considering the latter, IDFI requested judicial acts in a manner designed to avoid the possibility of refusals based on state secret or personal data protection concerns.

4.1. REGISTRY OF COVERT INVESTIGATIVE ACTIONS

The Supreme Court of Georgia is responsible for collecting and processing statistics related to motions, resolutions, and adopted legal acts regarding covert investigative actions by the common courts. According to paragraph 1 of Article 143^{10} of the Criminal Procedure Code of Georgia, "The Supreme Court establishes a register of secret investigative actions, which includes statistical information on covert investigative actions, in particular: information on motions filed with the courts for the carrying out of covert investigative actions, and on ruling rendered by courts on those motions, as well as information on the destruction of materials obtained as a result of operative-investigative actions…"

IDFI requested various public information from the Supreme Court of Georgia regarding covert investigative actions and measures stipulated in

Law “On Counter-Intelligence Activities”, categorized by different substantive, qualitative, and quantitative aspects. Namely, IDFI requested statistics on the review of motions/resolutions on covert investigative actions conducted by urgent necessity by common courts for the years 2021, 2022, and 2023, including data on the granting rates for each court, the types of investigative actions, and the relevant articles (crimes) of the Criminal Code. On top of that, the information on the prolongation of covert investigative actions, postponements of notification, and the destruction of obtained materials. In addition to these statistical data, IDFI also requested all legal acts (legal sources), methodology, and all official documents regulating the registry of covert investigative actions.

The Supreme Court of Georgia rejected IDFI's public information request. The court's response only provided a general statement indicating that the requested information is available on the Supreme Court's website. As for the information on the electronic surveillance measures and the regulatory act(s) of the registry of covert investigative actions, the mentioned issue remained unanswered *(Letter of the Supreme Court of Georgia dated May 24, 2024 N ჳ-386-24)*.

IDFI appealed the Supreme Court's response through an administrative complaint. According to the decision of the Supreme Court, the complaint was granted partially *(Decision of the Manager of the Supreme Court of Georgia of June 26, 2024 N ჸ-251-24)*. **Regarding regulatory acts of the Registry of covert Investigative actions, it was noted that The Supreme Court has not adopted any kind of such order/methodology, or other guidelines.** In this regard, the sole legal source is Article 143^{10} of the Criminal Procedure Code of Georgia. Regarding the statistics of covert investigative actions, the person responsible for the release of public information of the Supreme Court was obliged to provide these statistical data. The part of the complaint concerning electronic surveillance measures for counter-intelligence purposes was not granted *(see Chapter 3.2.8).*

4.2. AN ATTEMPT TO EVALUATE THE EFFECTIVENESS OF JUDICIAL OVERSIGHT: FIRST INSTANCE

One aspect of IDFI's public information requests referred to judicial acts related to covert investigative actions, namely rulings on granting authorization for these actions, decisions on the legality/illegality of urgently conducted measures, and decisions of the Court of Appeals assessing the lawfulness of the appealed covert investigative actions.

In this context, IDFI aimed at evaluating the effectiveness of judicial control over covert investigative actions, as well as assessing how well the court's legal argumentation aligns with human rights law and international standards, examining the standard of proof used by the court and determining the balance the court maintains between constitutional interests.

In order to examine/evaluate the above-mentioned issues, IDFI submitted public information requests to four city courts operating in Georgia (the City Courts of Tbilisi, Rustavi, Batumi, and Kutaisi). Additionally, two requests for public information were sent to the Tbilisi and Kutaisi Courts of Appeals.

4.2.1. REQUESTS SENT TO COURTS OF FIRST INSTANCE

On April 23, 2024, IDFI sent public information requests to four city courts. Generally, given the specific nature (secrecy) of covert investigative actions, there is a special regime for proceedings and case materials in first-instance courts. However, IDFI's statements were formulated in such a way that not all judgments were requested in a broad sense, but only the judgments where the need for secrecy of investigation and/or any other legitimate interest was disproved and/or where any state secrecy seal on the judgment had been lifted on one or other bases (due to reasons such as expiration, automatic revocation, end of investigation, destruction of information, notification of addressee, or other grounds for removing confidentiality etc.).

IDFI's requests contained a special indication that considering the time needed for information collection and processing, as well as the human resources involved, the applicant was willing to receive the information at an agreed-upon periodicity, even if this extended beyond the maximum period for public information issuance stipulated by the General Administrative Code of Georgia. The rulings were requested without any personal data and other identifying information.

4.2.2. POSITION OF COMMON COURTS

IDFI’s request was not satisfied by any of the courts. In all four cases, the legal argumentation was identical — a blanket refusal with only a general reference to the Law of Georgia “On State Secrets.” The courts deemed all the rulings sought by IDFI to be state secrets. There was an exception with the Rustavi City Court, which stated that specific types of acts (actions carried out with urgent necessity declared as illegal and actions where the information was destroyed due to the inadmissibility of the evidence obtained from covert investigative action) were never adopted by the court, while for the other rulings, the Court refused to issue them, referring to the state secrets.

None of the answers provided the details of the requisites of classification marking - the legal basis that confirms the classification of the information as secret in accordance with the procedures established by law (including the date of classification, classification level, and terms). Even if such legal acts existed, IDFI left the space for the courts to separate this particular information on the basis of state secrets and issue only those rulings that are not or are no longer, classified as state secrets.

The project team appealed the responses of Tbilisi and Rustavi city courts with administrative complaints on May 28, 2024. During the oral hearing of complaints, both courts' arguments essentially repeated the positions stated in their letters of refusal to provide public information.

Even on a legal hypothetical level, the courts considered it practically impossible to access these types of rulings, regardless of the expiration of the term of secrecy or other objective circumstances (such as achievement/exhaustion of the purpose, protected by state secret), unless the person has a special admission granted by the Law “On State Secrets” and/or the prosecutor’s office has adopted a special act on declassification of this information. In other words, the court has abstractly extended the protection of state secrets to all rulings on covert investigative actions, including the acts that must be declassified according to the law.

As for the security classification marking and its requisites, during the oral hearing of administrative complaints, the representatives of the courts were unable to provide information regarding the details of security classification marking and the terms of secrecy. There was only a general indication that such cases are considered under "secret proceedings."

It should be noted that both Tbilisi and Rustavi City Courts named the Prosecutor’s Office as the body fully responsible for the storage/classifying of court rulings and issuance of them. At the oral hearing, the representative of Rustavi City Court additionally noted that the court periodically requests declassification of its rulings from the Prosecutor's Office. During the hearing, the party presented the last such letter sent from the Rustavi City Court to the Prosecutor's Office, which requested the removal of the classification marking on dozens of documents. However, as the representative of the court noted, the Prosecutor's Office typically does not respond to these letters, leaving the court unaware of whether these documents remain classified or not. Additionally, it's important to mention that, parallel to the common courts, IDFI requested these judicial acts from the Prosecutor’s Office as well. In a letter dated April 25, 2024, No. 13/28095, the Prosecutor's Office informed IDFI that we should address the courts in order to receive the rulings delivered by the courts.

Both appeals had the same legal result, they were not granted.

4.2.3. LEGAL ASSESSMENT

The legal position of common courts to abstractly (generally) extend the protection of state secrets to the depersonalized texts of rulings, whose legal value in achieving criminal procedural and/or other legitimate purposes, has already expired, is not in compliance with the requirements provided by law and factually negates any possibility of making known to the general public the legal standards/arguments used by the courts regarding covert investigative actions.

Generally, state secret is indeed a legal interest that is worth protecting, however, the mentioned protection is limited to the legitimate interest for which the information is kept secret and to the terms established by the law. The process of maintaining information classified is strictly governed by the principle of legality. According to the first paragraph of Article 8 of the Law of Georgia “On State Secrets”, the classification of information as a state secret must adhere to the principles of legality, justification, and timeliness. The acknowledgment of information as a state secret is confirmed by the individual administrative act issued by an authorized person, which must include the necessary requisites such as the date, the level of secrecy, and a complete description of the information which is marked with classification marking.

Based on the principle of legality, it is not allowed to impose restrictions on information that does not fall into the standard of “as provided by law” - the law does not permit using “state secret” as a general/abstract basis for the closure of information.

Information is considered a state secret on specific grounds and to protect a specific legitimate interest. In the case of covert investigative actions, the legal purpose for conducting court hearings at closed sessions, as well as “closure” of all case materials, including judicial acts, is to ensure the effective investigation of a criminal case - stemming from a covert nature of actions.

Common courts extend the protection of state secrets to decisions where any legitimate interest, in terms of legal logic, has already expired, and the information, by its nature, should no longer be classified as a state secret.

Namely, through public information requests, IDFI requested the rulings on the cases where either the legal proceedings have been completed, the person has already been notified about the covert investigative actions, the obtained information has been destroyed due to being found unlawful/inadmissible or due to the other reasons, there was no longer ground for the information to be protected as a "state secret".

Regarding the court's claim that it has no influence over the classification of judgments and that this falls entirely within the authority of the prosecutor's office, the Criminal Procedure Code of Georgia specifies that one of the mandatory elements of a court judgment is a classification marking *(CPCG, Article 143³.10)*. It is impossible for the court not to be aware of the date, level, and term of the decision's classification.

According to the Law of Georgia "On State Secrets," the primary reason for declassification is the "expiry of the established term of secrecy" *(Law of Georgia on State Secrets, Article 16.1.c).* Additionally, before the expiration of this term, the law stipulates declassification due to "a change in the factual circumstances as a result of which it is no longer necessary to protect the information that is a state secret" *(Law of Georgia on State Secrets, Article 16.1.b).* In the latter case, the primary authority to declassify information is at the hands of a body that classified the information (the court), and in terms of covert investigative actions, also at the hands of a prosecutor *(Law of Georgia On State Secrets, Article 17.4)*. In other words, passing full responsibility by the court to the Prosecutor's Office in this process is unlawful. Even if all judgments were later declassified by the prosecutor's office "due to the objective circumstances," there are still judgments held by the court for which the maximum terms of every proceeding or classification have expired and do not require any additional act from a prosecutor.

Therefore, the court unlawfully restricts access to the texts of rulings that are beyond the period of limitation and are irrelevant for investigative purposes. By unjustified use of the Law of Georgia “On State Secrets,” the court abstractly (generally) prohibits access to these rulings in any form and/or extent.

4.3. AN ATTEMPT TO EVALUATE THE EFFECTIVENESS OF JUDICIAL CONTROL: THE SECOND INSTANCE

IDFI also sent requests to the Tbilisi and Kutaisi Courts of Appeals. Unlike the courts of the first instance, in this case, no specific formulation was chosen - related to the final decision on the case and/or the addressing potential risks of state secrets. IDFI requested the last five court decisions on recognition of first instance court ruling on covert investigative action lawful/unlawful (without personal data and other identifying information).

This approach was based on the specifics of the grounds and procedure in the appeals instance. Specifically, the hearing of a case in the Court of Appeals concerning covert investigative actions is preceded by a complaint of an informed (notified) individual about the covert investigative action - when a person learns about covert investigative action against him/her during or after the proceedings and appeals its results, seeking the restoration of the right to privacy and challenging the admissibility of the evidence obtained from the investigative action.

Therefore, at the level of the court of appeals, the need to protect the judgment under state secrecy to ensure the effectiveness of the investigation and the secrecy of the investigative action is no longer relevant. Moreover, the latter is even repeated in the provisions of the Criminal Procedure Code of Georgia. Specifically, in the court of appeals, the general rules of case hearing apply - namely, during open court sessions with parties invited. Paragraph 16 of Article 143^3 of the Criminal Procedure

Code of Georgia directly indicates that decisions on complaints must be announced publicly.

Neither the Tbilisi nor the Kutaisi Court of Appeals have provided the requested decisions. In both cases, the response was identical - a general reference to the Law of Georgia "On State Secrets."

IDFI filed an administrative complaint against the refusal of the Tbilisi Court of Appeals. The requested information was not provided to IDFI as a result of the complaint as well. However, during an oral hearing, the court representatives noted that the appeals related to covert investigative actions **are filed and heard "in camera" in a closed session. During the complaint review process, IDFI learned that the Court of Appeals, when handling appeals related to covert investigative actions, applies a procedure that is used in the first instance, (hearing the case in a closed session).**

According to the court, since the Criminal Procedure Code of Georgia does not explicitly state that appeals in the Court of Appeal must be heard in an open session, the legislation "does not oblige the court to open the session", and therefore, the court follows Paragraph 5 of Article 143^3 of the Code, which outlines the general rule for the first instance court proceedings.

The initiator of proceedings on covert investigative actions in the Court of Appeals is a person who either after the end of the proceedings was informed by the prosecutor about the covert investigative actions carried out against him/her and had the right (procedure) to appeal explained, or received this information from another source. The dispute in the court of appeals concerns only the legality/illegality of the action and the potential violation of the person's right to privacy. At this stage, the interest protected as a state secret — ensuring the covert nature of the investigative action — has already expired.

Even formally, after the conclusion of the legal proceedings, it is impossible for a person's notification of a covert investigative action not to be preceded

by a change of the state secret regime based on a relevant legal act, whether delivered by the prosecutor's office or the court.

Furthermore, this rationale is even confirmed by the Criminal Procedure Code, through setting different procedures of case considerations for either the first instance courts and the courts of appeals. Paragraph 5 of Article 143^3 of the Code stipulates that motions for covert investigative actions must be reviewed in a closed court session, and the decision must be made in four copies and delivered to the subjects defined by law. In contrast, Paragraph 15 of Article 143^3 of the Code requires that a court of appeal shall, by notification, ensure the participation of the appellant and the prosecution in the review of the appeal, and a decision made on the appeal shall be publicly announced.

The court cannot arbitrarily extend the rule of closed court sessions to cases not directly stipulated in the law. The Court of Appeals' interpretation — arguing that as Paragraph 15 of Article 143^3 of the Code does not explicitly require an open session for appeals and thus applying the closed hearing procedure set for the first instance courts — appears to contradict the principle of legality. This approach illegitimately broadens the grounds for the closure of court sessions.

4.4. AN ATTEMPT TO EVALUATE THE EFFECTIVENESS OF JUDICIAL CONTROL OVER COUNTER-INTELLIGENCE ACTIVITIES

Within the framework of the project, the second category of judicial acts requested as public information were the orders of the Supreme Court concerning permission for electronic surveillance under the Law of Georgia “On Counter-intelligence Activities.” Given that motions for these orders are typically reviewed by the supervising judge of the Supreme Court in a closed session, and the documents related to the issuance of permission for electronic surveillance (motions, orders, etc.) are subject to state secrecy legal regime, IDFI requested orders that:

1. Are not marked with classification marking as provided in the Law of Georgia “On State Secrets” and/or the term of classification had expired at the moment of submitting the application on public information;

2. A person was notified about operational-technical measures against him/her in accordance with the Law of Georgia “On counter-intelligence activities."

IDFI's request was limited to the orders (without personal and other identifying data - only the legal justification) for which the legal basis for protecting state secrecy no longer existed and, formally, the requested orders no longer have been recognized as state secret by the issuance of a special act on their declassification.

The Supreme Court of Georgia, citing the Law of Georgia "On State Secrets," refused to provide the requested information.

IDFI appealed the Supreme Court's response in an administrative manner. However, the Supreme Court's position remained unchanged during the review of an administrative complaint. Moreover, the court representatives noted that the period of classification might not be mentioned in the judge's order at all, as "due to objective circumstances," it is impossible to determine the duration of this action in advance.

According to the Law of Georgia "On State Secrets," one of the main principles regarding protecting secrecy is timeliness. Information can be classified as state secret only “in accordance with the law”, for a specific term (defined by the law as well), and to achieve a specific legitimate goal. The Supreme Court applies an abstract (general) classification rule and unjustifiably restricts the right to access public information.

Regarding the Supreme Court's claim that it is impossible to determine when the term of classification for an order will expire, it should be noted that both the Law of Georgia "On State Secrets" and the Law "On Counter-intelligence Activities" are strictly bound by the principle of timeliness. The

law allows electronic surveillance only for the period necessary to achieve its purposes, but not more than 90 days. This period can be extended only in exceptional cases, in the same manner, and on the same basis as the initial order, each time not exceeding 12 months. In any case, the decision to extend the term is made in the same manner and by the same institution (the supervising judge of the Supreme Court). In other words, it is impossible for the court not to have information or access to orders whose legal terms of classification have completely expired. Practically the court has blocked a way for the public to be informed about the legal standards applied by the court, even through the availability of the earliest orders.

The research revealed that even fully using administrative proceedings and the administrative complaint mechanism, it is practically impossible to obtain acts of judicial control over covert surveillance from the court system (and not only from the court system) (as mentioned earlier, in addition to requesting copies of the rulings from the common courts, IDFI requested them from the Prosecutor's Office as well).

This is referring only to those acts that no longer have legal value for investigative, state security, or other purposes and should no longer be protected as state secrets. Through both the formulation of requests and the effective use of administrative complaint mechanisms, IDFI tried to minimize potential legal risks associated with obtaining judicial acts on covert surveillance. Nevertheless, even using all possible mechanisms at the administrative stage, obtaining acts of judicial control over covert surveillance in any form and/or extent remains ineffective.

IDFI's observation showed that, contrary to the requirements of the law, the state secret protection regime (both *de facto* and, in some cases, *de jure*) is widely applied to these acts. This makes it impossible to access even the earliest acts, whose protection value is undoubtedly expired. The practice of concealment of these acts and the legal standards used by the courts/Prosecutor’s Office significantly contradict the right to receive public information and make it practically impossible to assess the substantive part of judicial oversight exercised over covert surveillance activities.

5. CONTROL THROUGH ELECTRONIC SYSTEM

The technical capabilities of obtaining information play an important role, including in understanding the functioning of the mechanism of external control over its implementation. For example, in terms of obtaining communication in real-time, as well as accessing the information in the data identification bank or during the real-time geolocation identification, the legislation provides/should provide the possibility of monitoring and, if necessary, active intervention by the state authorities exercising such control through the electronic system that is used during these activities. The supervising judge of the Supreme Court of Georgia is equipped with such functions during the actual implementation of electronic surveillance for counter-intelligence purposes and the Head of the Personal Data Protection Service (hereinafter - the Head of Service) in relation to the covert investigative measures. This chapter reviews these both control functions and their possible scope.

5.1. THE CONTROL EXERCISED BY THE HEAD OF SERVICE

In the process of carrying out covert investigative actions, from a technical point of view, three types of electronic systems are created by legislation: obtaining communications in real-time, accessing the information in the data identification bank, and implementing real-time geolocation identification. However, the principle of technical operation of each, at least from the point of view of control over them, is essentially identical.

From a technical point of view, there are two electronic control systems incorporated in the electronic system for the implementation of covert surveillance measures - electronic control and special electronic control systems *(Law on Agency, Article 2. "i", "j").*

Namely, a ruling on authorization of covert investigative action or a resolution of a prosecutor (as well as a ruling of a court on authorization/denial of authorization of a resolution) is forwarded by the

relevant investigative body to the Agency in material form. Parallel to this, the same documents are forwarded to the Head of the Personal Data Protection Service in the same form. The Agency starts implementing covert investigative actions upon receiving a ruling or a resolution *(Law on Agency, Article 13. "a", CPCG, Article 143[3].5,6[2]).*

Different procedure is provided for covert eavesdropping and recording of telephone communication, where the commencement of the action by the Agency requires an additional stage, and the electronic control system serves to ensure this stage. In particular, after receiving a decision/resolution in a material form, the Agency ensures that these documents are provided to the Head of the Personal Data Protection Service through an electronic form, through the electronic system, organized for obtaining information in real-time. It is the latter's confirmation of receipt of the electronic copy that creates freedom for the Agency to begin eavesdropping/recording of telephone communication *(CPCG, Article 143[3].5[1],6[2])*.

By this time, the Head of the Personal Data Protection Service has gathered the material and electronic copies of the rulings/resolution, respectively, received from the Prosecutor's Office and the Agency (through an electronic system), and upon comparing them and identifying the ambiguities or inaccuracies, he/she can suspend a covert investigation action until the removal of the ambiguities or inaccuracies (*CPCG, Article 143[3].5[4],5[5]; 143[6].5."e").* Moreover, a covert investigative action may be suspended by the head of the Personal Data Protection Service in the cases when a ruling/resolution on authorization of covert eavesdropping of telephonic communication is not provided to him/her in material or electronic form.

The Personal Data Protection Service, in its current configuration, started exercising its powers on March 1, 2022, after the widely criticized so-called reform of the State Inspector Service. These functions were carried out by the State Inspector Service until March 1, 2022. Unfortunately, the Personal Data Protection Service provided IDFI with statistical data on its activities related to covert investigative actions only for the period after March 1,

2022. The reason for this is unknown, but it is a fact that the principle of continuous processing/disclosure of statistical data has been breached.

According to the information provided by the Personal Data Protection Service, in the period from March 2022 to December 2023, the following acts were submitted to the service regarding covert investigative actions:

DOCUMENT	ACTION	2022	2023
COURT RULING ON COVERT INVESTIGATIVE ACTION	Covert eavesdropping and recording of telephone communication	1077	859
	Video and/or audio recording, photographing	888	1022
	Retrieval and recording of information from a communications channel	4	3
	Collecting Internet traffic data	0	1
PROSECUTOR'S RESOLUTION ON CONDUCTING COVERT INVESTIGATIVE ACTION IN THE CASE OF URGENT NECESSITY	Covert eavesdropping and recording of telephone communication	51	16
	Video and/or audio recording, photographing	99	76
COURT RULING ON PROLONGING A COVERT INVESTIGATIVE ACTION	Covert eavesdropping and recording of telephone communication	288	228
	Video and/or audio recording, photographing	186	122

As for the use of the mechanism of addressing ambiguities or inaccuracies, Service used this mechanism 14 times in 2022 (from 01.03.2022), and 6 times in 2023. As for the suspension of covert investigative actions, the Service suspended 252 actions.

LEGAL GROUND	2022	2023
Delay of court ruling	169	74
Declaring the covert investigative action carried out by the prosecutor's resolution as partially illegal	3	0
Declaring the covert investigative action carried out by the prosecutor's resolution as illegal	2	1
Removal of ambiguities or inaccuracies in a court ruling	1	0
Termination of a covert investigative action	1	1

Besides the above-mentioned activities, carried out through an electronic system, the Personal Data Protection Service controls the implementation of covert investigative actions and the processing of data during these actions through the inspection. The inspection implies the examination of the lawfulness of data processing *(Article 49, "c" of the Law of Georgia On Personal Data Protection)*, and is applied to all of the actions subject to the study under this report *(Article 54.1."c",2-6 of the Law of Georgia On Personal Data Protection)*.

Based on the information provided by the Personal Data Protection Service, in the period from March 1, 2022 to December 31, 2023, the LEPL Operative-Technical Agency of Georgia was inspected two times:

- In 2022, 1 (one) unplanned inspection was carried out, related to a covert investigative action - covert eavesdropping and recording of telephone communication. As a result of this examination, the fact of administrative offense was not revealed, however, 2 (two) mandatory instructions were addressed to the Agency;

- In 2023, 1 (one) planned inspection was carried out, related to a covert investigative action - covert video and/or audio recording, photographing. As a result of this examination, the fact of administrative offense was not identified.

During 2022, the Personal Data Protection Service was addressed by 93 persons, requesting information on whether or not they were subject to covert investigative actions. The Personal Data Protection Service — through the examination of submitted documents and the application of electronic systems, studied these requests and none of the facts were revealed that would create grounds for the obligation to notify a person based on Article 143^{9} of the Criminal Procedure Code.

In 2023, 4 persons addressed the Personal Data Protection Service, requesting information on whether or not they were subject to covert investigative actions. In one case, based on the statement submitted, the Service examined the alleged violation of notifying an applicant by the Prosecutor's Office of Georgia, as well as the latter's obligation to submit a record of destroying the evidence obtained through covert investigative actions. In this case, based on the examination of the Prosecutor's Office, the fact of administrative offense was not identified.

Additionally, in 2023, the Personal Data Protection Service inspected the Special Investigation Service and the Operative-Technical Agency. The inspection of the Special Investigation Service involved the examination of the fulfillment of the obligation provided for by Article 143^{6}, paragraph 14 of the Criminal Procedure Code - to submit a protocol drawn upon completion of a covert investigative action. As a result of an inspection, the Special Investigation Service was subject to administrative liability based on the Law of Georgia "On Personal Data Protection Service" and was addressed by one instruction to be met.

5.2. THE SUPREME COURT OF GEORGIA

The supervising judge of the Supreme Court of Georgia controls the covert surveillance measures conducted for counter-intelligence purposes, using practically identical technical means. Namely, the supervising judge has the authority to remotely suspend eavesdropping of telephone communication, in the cases when the material and electronic documents, giving grounds

for covert surveillance, are incompatible with each other, contain inaccuracies, or the judge was not provided with an electronic copy *(The Law on Agency, Article 2. "i")*.

Unlike eavesdropping, carried out as part of covert investigative action, the legislation on counter-intelligence activities does not provide for a restriction that secret surveillance measures can commence only after the confirmation of receiving an order/decision by the supervising judge *(Law on Counter-Intelligence Activities, Article 14[1].1).*

It is worth noting that, if a decision on carrying out covert investigative actions is made by a judge (including, through post-factum authorization of a prosecutor's resolution), and the technical control is carried out by the Head of Service, in terms of counter-intelligence activities, these both functions are under the supervising judge of the Supreme Court of Georgia.

Furthermore, it should be noted that it is not clear from the legislation whether the functions of the supervising judge are assigned to one or more judges. In addition, it is impossible to determine whether the judge has the authority to access the above-mentioned electronic systems and perform the relevant actions directly, or whether he/she is authorized to entrust the technical execution to a specific authorized person(s). And, in the case of direct control by him/her, to what extent the supervising judge is equipped with relevant technical skills.

As mentioned above, no information regarding counter-intelligence activities could be obtained from the Supreme Court, including information that should not be declared as a state secret. Therefore, we are unable to assess the effectiveness of the technical or substantive control of the Court over counter-intelligence activities.

6. DOCUMENTED INCIDENTS OF COVERT INVESTIGATIVE ACTIONS AND THE STATE'S RESPONSE TO THEM

6.1. THE COMPETENCE OF THE SPECIAL INVESTIGATION SERVICE

Since March 1, 2022, violation of the right to privacy in private communications, as well as other crimes under Articles 157-159 of the Criminal Code, falls under the investigation competence of the Special Investigation Service (SIS). IDFI requested statistical data from the Special Investigation Service referring to the aforementioned crimes from March 1, 2022, until the date of submitting the request.

ARTICLE OF CRIMINAL CODE	2022	2023	2024
Article 157. Disclosure of Information on Private Life or of Personal Data	17	4	2
Article 157[1]. Disclosure of Secrets of Personal Life	87	159	47
Article 158. Violation of the Secrecy of Private Communication	1	3	1
Article 159. Violation of Secrecy of Personal Correspondence, Phone Conversations or Other Kinds of Communication	9	10	2
Total Number of Criminal Cases	110	171	50

As of March 31, 2024, 244 cases were pending at the Special Investigation Service. Criminal charges were brought against 87 persons, and only 6 of them were the representatives of law enforcement agencies:

- Ministry of Defence 3;
- Security Police 1;
- Penitentiary Service 1;
- Ministry of Internal Affairs 1;

Since March 1, 2022, none of the accused law enforcement officers in cases under the jurisdiction of the Special Investigation Service are, under their competence, persons responsible for carrying out covert investigative actions and/or a representative of special agencies that carry out electronic surveillance within counter-intelligence activities.

6.2. STATE'S RESPONSE TO DOCUMENTED INCIDENTS: THE CASE OF SO-CALLED "DATA COLLECTIONS"

In 2021, materials depicting private communication and the personal lives of various individuals were repeatedly disseminated, raising legitimate concerns about systematic illegal covert surveillance. Particularly:

1. A recording was released, which allegedly depicted the personal telephone communication of Bera Ivanishvili and Irakli Garibashvili;

2. Allegedly a former SSSG employee claimed that orders were given to install surveillance equipment in the homes of various individuals, including politically active persons, to obtain footage of their private lives;

3. On September 13, 2021, media outlets were provided with thousands of allegedly illegally obtained files, which contained personal information, including private communications, information about crimes, and the private lives of various individuals, including clergy, lawyers, journalists, and diplomats (the so-called "Data Collections" case).

The purpose of this analysis is not to evaluate any specific incident; however, we deem it relevant to review the actions and responses from the relevant oversight institutions after this unprecedented leakage of data in the history of Georgia.

September 13, 2021 - a large volume of documentary material allegedly processed by the SSSG including through proceeding the information obtained via covert surveillance, was leaked online and sent to the media. The material was primarily in text format and exceeded 10 gigabytes in total size. According to the Public Defender, an unprecedented leakage of materials depicting covert surveillance took place on September 13, 2021. The Ombudsman stated that the volume of distributed documents reveals that the material was obtained as a result of allegedly illegal covert surveillance carried out by state authorities. The special report of the Public Defender indicates that the leaked materials contain various types of personal data including alleged information about sexual violence against minors, non-reporting of committed crimes, and abuse of power by law enforcement officials *(2022 report, p. 123)*. The release of these records also gathered international attention, being mentioned in the 2021 reports of the US State Department and Freedom House.

September 14, 2021 - the State Inspector Service issued a statement. SIS was the predecessor to the current Personal Data Protection Service which had the technical control mechanisms over the Agency of SSSG as described in this report. According to the Inspector, “the competence of the SIS ends where there are signs of crime. In addition, the supervisory powers of the State Inspector Service do not extend to the processing of personal data classified as a state secret for the purposes of security of the state, defense, intelligence, and counter-intelligence activities. Accordingly, SIS is deprived of legislative mechanisms and authority to investigate covert surveillance potentially conducted in violation of legislative requirements''. The statement highlighted that counter-intelligence activities were beyond the jurisdiction of SIS and urged the Constitutional Court to review in a timely manner the constitutional complaints filed by 326 citizens concerning the constitutionality of the existing covert surveillance infrastructure. According to the 2021 report of the State Inspector Service *(p. 291),* in relation to the so-called “Data Collections”, 22 individuals filed appeals to the State Inspector Service, claiming that their telephone communications were included in the leaked materials. They demanded the

response and verification of whether they had been subject to surveillance. The SIS determined within its authority that no covert surveillance measure had been carried out against any of them, which would raise the obligation of notifying the individuals involved. Accordingly, the appeals were forwarded to the Prosecutor's Office of Georgia for further action.

September 14, 2021 - The Prosecutor's Office of Georgia launched an investigation on the fact of the dissemination of materials under paragraphs 1 and 2 of Article 158 of the Criminal Code (violation of the secrecy of private communication) with all necessary investigative actions.

September 14, 2021 - The State Security Service issued a statement and stated that the Service was ready to cooperate with the Prosecutor's Office of Georgia as conducting a comprehensive and extensive investigation was in the interests of both institutions.

September 18, 2021 - The Prosecutor's Office issued a statement and indicated that far-reaching investigative measures were in progress, which included addressing the United States for international assistance.

September 18, 2021 - The Public Defender of Georgia appealed to the UN Special Rapporteur on the right to privacy and the Parliament of Georgia to conduct an in-depth investigation on this matter. At the same time, the Public Defender requested, as an exception, access to the investigative materials from the Prosecutor's Office. It becomes evident from the report of the Public Defender for 2021 that this request had been denied by the Prosecutor's Office *(Public Defender's report p. 161)*.

April 23, 2024 - IDFI addressed the Prosecutor's Office of Georgia and requested information about the ongoing proceedings regarding the "Data Collections" case. Specifically, IDFI requested data on the number of individuals being criminally prosecuted, including relevant articles and dates, the number of law enforcement representatives involved, the outcomes of criminal prosecutions, the use of measures of restraint, judgments, and the overall progress of the case.

The Prosecutor’s Office responded, indicating that the investigation is conducted under paragraphs 1 and 2 of Article 158 of CCG, as well as sub-paragraph “A” of paragraph 4. A total of 118 individuals have been recognized as victims.

The so-called “Data Collections” incident clearly demonstrated that the covert surveillance system in Georgia poses a significant threat not only to individuals’ rights but also to the democratic and legal state in general. Despite the unprecedented scale of the incident, its investigation is delayed indefinitely. The State Inspector Service (now the Personal Data Service) indirectly recognized the ineffectiveness of its own mandate and pointed to other institutions, including the Constitutional Court, which has been reviewing the constitutionality of existing technical capabilities of covert surveillance for over seven years. Despite these issues, the main mechanism of Parliamentary control over the “Data Collections” incident - the investigative commission - was not created.

7. CONTROL POWERS OF THE PARLIAMENT OF GEORGIA: POLITICAL AND LEGAL OVERSIGHT

While discussing external control mechanisms over the Agency's activities, the Parliament of Georgia plays an important role in this regard. The Parliament exercises control over the agency through parliamentary oversight mechanisms *(Law on the Agency, Article 24.1).* These mechanisms include for example, questions of the MPs, interpellation, and the Minister's hours. Specifically, regarding covert surveillance measures, the most crucial Parliamentary mechanisms include the Trust Group and the Temporary Investigation Commission.

7.1. TRUST GROUP

The Trust Group is a parliamentary control mechanism established in the Defence and Security Committee of the Parliament of Georgia. Its objective is to oversee state institutions within the defense and security sector, including the Agency *(Rules of Procedure, Articles 156, 157.1).* The Trust Group shall be composed of five members, including the Chairperson of the Defence and Security Parliamentary Committee, and representatives from both the parliamentary majority and opposition *(Rules of Procedure, Article 157.2).*

It is important to note that the Trust Group's control functions are limited to reviewing activities related to counter-intelligence purposes and do not extend to covert investigative actions carried out for criminal procedure purposes *(Law on the Agency, Article 24.1).* Therefore, its control functions encompass only the activities carried out for counter-intelligence purposes.

The Trust Group can supervise secret activities and special programmes in the field of the defense and security of Georgia in accordance with the procedure established by the legislation of Georgia, except for aspects related to secret forms and methods of activity *(Rules of Procedure, Article 159.1)*. The Trust Group is entitled to request any information necessary for

the fulfillment of its functions. However, there is an exception for the Agency. The Rules of Procedure sets separate regulations for the Agency and its obligation, regarding providing of information, is only limited to submitting an annual (not later than 15 April) statistical and generalized report *(Rules of Procedure, Article 159.2,9; Law on the Agency, Article 24.2).*

The Trust Group, within its mandate, has the authority to check the secret activities and special programs of the relevant agency, however, this authority does not extend to information related to the secret forms and methods of activity *(Regulations, Article 159.1)*. The activity of the Trust Group, in general, implies its authority to request from the relevant agency any information that the latter needs for the full implementation of its functions. However, within the framework of this rule, we exceptionally find a reference to the agency's obligation to provide information to the Trust Group, which implies that the agency does this only by providing an annual (no later than April 15 of the following year) generalized report and statistical information *(Rules of Procedure, Article 159.2,9; Law on Agency, Article 24.2)*.

Besides this, the Agency is obliged to proactively introduce to the Trust Group secret normative acts containing the “main goals of the structure of an agency and the structural units of an agency” *(Rules of Procedure, Article 159.7)*.

One oversight measure within this Parliamentary control mechanism is the authority to conduct visits to relevant agencies, including the Agency, and interview employees; and study the information related to the Agency’s activities. The agency is notified of such visits in advance. The Trust Group can inspect the agency no more than twice a year *(Rules of Procedure, Articles 159.11,12)*.

Additionally, the Trust Group has the authority to oversee budgetary expenditures, including secret state procurement, by receiving information about individual purchases above a specified amount and the general information on all such purchases *(Rules of Procedure, Articles 159.5,6)*.

This overseeing function is applied to all institutions within the Security and Defense sector, as well as the Agency in particular.

IDFI requested various information related to the Trust Group's activities for 2021, 2022, and 2023 from the Parliament of Georgia. The requested information included the number of sessions held, attendees, minutes of each session, cases of addresses to and information requests from the relevant institutions, cases of inspections of the Operative-Technical Agency, recommendations addressed, and the state of their implementation.

During the reporting period, the Trust Group held 46 sessions: 16 in 2021, 16 in 2022, and 14 in 2023.

During 2021, the Trust Group of the Parliament of Georgia requested information from the following state institutions: the Ministry of Internal Affairs of Georgia (once), the Intelligence Service of Georgia (3 times), the State Security Service of Georgia (8 times), the Operative-Technical Agency (9 times), the Special State Protection Service of Georgia (once). In 2022, the Trust Group requested the information from the SSSG’s Agency 7 times. According to the information provided by the Parliament, the answers were provided in a timely manner. During the reporting period, the Trust Group of the Parliament of Georgia made a decision to inspect the agency 3 times.

Regarding the statistical information about addressing relevant law enforcement bodies by the Trust Group, in cases of detecting signs of crime, statistics of addresses to the head of the State Security Service or the Prime Minister in cases of illegal and unjustified classification of information, as well as the recommendations issued to the Operative-Technical Agency and the state of their implementation, the mentioned issues remained unanswered by the Parliament. Generally, the Parliament of Georgia did not provide any information about the actual results of the activities of the Trust Group.

Regarding the request to provide the minutes of sessions of the Trust Group as public information, the Parliament of Georgia referred to Article 158 of

the Rules of Procedure of the Parliament of Georgia, according to which, sessions of the trust group shall be closed and the Parliament is "deprived of the opportunity to send the requested minutes". To seek any kind of report regarding the Group's activities, the Parliament of Georgia referred us to its website. The only document/report regarding the results of the Trust Group's activities, reflecting the work of the Trust Group for 2021-2023 and is published on the website is available here - link.

7.2. TEMPORARY INVESTIGATION COMMISSION

Article 42 of the Constitution of Georgia allows for the creation of a Temporary Investigation Commission by the Parliament in the presence of information on the illegal acts or corruption offenses of state bodies and officials that threaten state security, sovereignty, territorial integrity, or the political, economic or other interests of Georgia *(Rules of Procedure, Article 61.2.a*). The commission is established to investigate specific issues and is dissolved upon completion of its investigation *(Regulations, Articles 67.1, 4, 5, 6, 12).*

Attendance at the sittings of a temporary investigative commission at its request shall be mandatory. Furthermore, if requested by a temporary investigative commission, state bodies, officials, and natural and legal persons shall, within the time limit determined by the commission and in accordance with the established procedure, submit the conclusions required for the examination of the issue and other necessary materials. The Commission can also request to be familiarized with criminal case materials. To ensure effective functioning, the commission can form a working group comprised of commission members and invited experts *(Regulations, Articles 67.1, 4, 5, 6, 12).*

From a point of view of results, after the study of the issue, the temporary investigation commission is authorized to address the Parliament both with a proposal to collect signatures for raising the issue of impeachment against the relevant officials, and in the presence of necessary information, address

“relevant body or official responsible for preventing a violation of the legislation of Georgia, and, depending on the nature of the violation of the legislation of Georgia, raise the issue of initiating an investigation, bringing administrative or disciplinary proceedings, reclaiming state property from illegal possession, or deciding on compensation for damage caused to the State” *(Regulations, 67.11;70.1)*.

Also, the results of the investigation commission's work can become the basis of political and/or legal responsibility of a relevant person, which may also imply raising an issue of impeachment. The temporary investigation commission was never created in response to covert wiretapping, including the so-called “Data Collections” incident.

8. EFFECTIVENESS OF CONSTITUTIONAL CONTROL OVER THE LEGISLATION ON COVERT SURVEILLANCE MEASURES

According to paragraph 2 of Article 59 of the Constitution of Georgia, constitutional control is conducted by the Constitutional Court of Georgia. Within its competence, the Court has the authority to assess the constitutionality of normative acts, which may result in declaring such acts unconstitutional and invalid.

Thus, all normative acts, including those regulating issues related to covert surveillance measures, are subject to constitutional review. In this process, the Constitutional Court possesses the power to conduct a comprehensive examination to determine whether the disputed legislation poses a significant risk of misuse that is inconsistent with the Constitution. In this regard, the Court is able to obtain any necessary information for the assessment, including confidential information.

In the Georgian legal reality, challenging the constitutionality of legislation regulating covert surveillance measures before the Constitutional Court is not a novel concept. The Court's case law includes multiple cases, both pending and adjudicated, addressing this issue.

8.1. JUDGMENT OF THE CONSTITUTIONAL COURT OF GEORGIA ON THE CONSTITUTIONAL COMPLAINT N625,640: UNCONSTITUTIONALITY OF DIRECT ACCESS TO TELECOMMUNICATIONS INFRASTRUCTURE

Initially, the Public Defender and the non-governmental organizations participating in the "This Affects You Too" campaign appealed to the Constitutional Court of Georgia on February 3, 2015, and April 15, respectively. The claimants appealed the norms regulating covert surveillance, which included a two-stage electronic system (referred to as the two keys and permanent connection) for executing covert investigative actions, and requested them to be declared unconstitutional.

Shortly after addressing the Court, on June 26, 2015, the Constitutional Court confirmed the admissibility of constitutional claims. On April 14, 2016 (about 1 year after the appeal to the Court), the Constitutional Court upheld the claimants' request and declared several provisions of the Law of Georgia "On Electronic Communications" unconstitutional. The Court clarified that the State Security Service had a professional interest in accessing extensive information to aid the investigation process. Consequently, the continuous access of such a state body to relevant data and electronic communication processes unjustifiably heightened the risk of infringing individual rights.

It should be noted that in its aforementioned judgment, the Court deferred the invalidation of the disputed norms until March 31, 2017, giving the Parliament of Georgia a reasonable period for the adoption of the legislative amendments in compliance with the constitutional requirements.

On March 22, 2017, the Parliament of Georgia overrode the President's veto and adopted legislative amendments, thus establishing a new framework for the regulation of covert electronic surveillance. The citizens of Georgia, the Public Defender of Georgia, and the political parties appealed once more to the Constitutional Court in the framework of the campaign "This Affects You Too" for the evaluation of the constitutionality of the new legislative changes.

8.2. PUBLIC DEFENDER OF GEORGIA AND OTHERS: (A TOTAL OF 326 CONSTITUTIONAL LAWSUITS): CONSTITUTIONALITY OF TECHNICAL CAPABILITIES OF THE STATE SECURITY SERVICE

As already noted above, after the judgment of the Constitutional Court of Georgia dated 14 April 2016, in April and May 2017, the interested parties once again addressed the Court requesting to declare the above-mentioned legislative changes unconstitutional. It is noteworthy that the Court began its consideration of the case expeditiously; the executive session, which

included oral hearings, took place on June 20, 21, and 22, July 7 and 8, and September 7, 2017.

It is worth noting that the claimants in the case requested the invalidation of the contested norms at the executive session, arguing that the legislative amendments did not bring about any substantial changes. They argued that the challenged norms effectively circumvented the Constitutional Court of Georgia's judgment from April 14, 2016.

In its recording notice dated December 29, 2017, the Constitutional Court did not uphold the claimants' request to invalidate the disputed norms and decided to accept the case on its merits.

Substantive review on the matter came to an end on April 17, 2019. However, the Constitutional Court has yet to render a judgment on this matter. Consequently, the plenum of the Constitutional Court has been in deliberation for over five years in this case.

8.3. CONSTITUTIONAL COMPLAINT N690: CONSTITUTIONALITY OF THE NORMS REGULATING COUNTER-INTELLIGENCE ACTIVITIES

The aforementioned case is related to electronic surveillance within the context of counter-intelligence activities and has been pending in Court since November 16, 2015. The claimant argues that the lack of judicial review and the indefinite scope of authority concerning the use of covert video and audio recording, covert film and photography, television cameras, and other electronic devices are unconstitutional. The claimant argued that the disputed norms essentially replicate the regulations addressed in a previous judgment by the Court. Despite this, the Court did not concur with the claimants' position on declaring the challenged norms invalid without assessing them on merits. Consequently, the N690 constitutional claim was admitted for review on merits on November 25, 2016.

The review on merits of the mentioned case commenced on December 21, 2016; however, the defendant submitted a motion to close the court

session. As a result, the current status of the case remains unclear, though it is evident that more than seven years have passed since the beginning of its review on merits.

The analysis of ongoing cases before the Constitutional Court indicates that the Court has taken an excessively long time to render judgments on matters concerning covert surveillance. It is obvious that since around 2020, the Court has refrained from adjudicating such cases on the merits. Consequently, this situation suggests a negative evaluation of the Court’s effectiveness in handling covert surveillance cases.

CONCLUSION

Normative analysis of the covert surveillance measures actions, as well as the practical information obtained by IDFI, makes it evident that the Agency of SSSG is a service provider of covert surveillance measures for state institutions. The Agency has access to Georgia's communications infrastructure enabling it to install devices and software on it as well.

The current legislation provides a number of technical and normative mechanisms aimed at ensuring the lawful implementation of covert surveillance measures. These mechanisms could possibly be adequate for preventing the abuse of power of a dishonest employee; however, Georgia’s recent history shows that the problem is systemic illegal surveillance operations sanctioned by high-ranking officials, rather than “the risk of a dishonest employee”.

Considering this, it is crucial to ensure the transparency, accountability, and effectiveness of the state institutions involved in the external oversight of the security sector. Working on this report revealed that there is no sufficient information to assess the effectiveness of these institutions, and the scarcity and low quality of the received information do not allow to draw convincing conclusions about the effectiveness of external oversight mechanisms.

In terms of accountability, a significant challenge lies in the inadequate response of relevant authorities, including the Prosecutor's Office and Parliament, to publicly documented incidents. This inaction fosters the perception that systematic illegal eavesdropping or surveillance, including politically motivated operations, persists up to the present day.

Regarding the transparency of state institutions involved in the external oversight of covert surveillance measures, access to public information and quality statistical data is an essential challenge. These institutions frequently and grossly violate the constitutional right to public information.