Information prepared by the Office of the Personal Data Protection Inspector of Georgia

Legal Framework and Oversight Mechanisms of Surveillance in Georgia

Introduction

The value of personal data processing for investigation of organized crime, fight against terrorism and protection of national security is unquestionable, especially when it comes to secret surveillance, which is a particularly necessary tool for law enforcement authorities to fulfill their tasks.

At the same time, surveillance measures have a covert nature, which deprives individuals and public the ability to scrutinize this intrusive procedural power.

In these circumstances the role of the state is essential to provide necessary guarantees for the protection of fundamental rights. The major challenge is to establish a legal and technical system that ensures the efficiency of operations of relevant authorities and at the same time minimizes the risks of abuse and provides adequate protection of privacy. First and foremost is to adopt a legal framework that ensures that interference with privacy is legitimate, proportionate and necessary in a democratic society. Second and no less significant is to provide independent oversight mechanisms, that can successfully operate in practice and ensure accountability of relevant authorities.

The present document provides an overview of the Georgian legal framework on surveillance and relevant oversight mechanisms.

Legal Framework

Types of surveillance measures

Georgia operates a legal system which enables the investigation authorities to conduct the following surveillance measures:

- Interception of telephone communications;
- Interception of information from a communication channel or computer system and installation of software into the computer system for interception purposes;
- Control of the postal and telegraphic transfer;
- Covert video/audio surveillance and photo recording;
- Electronic surveillance through technical means.

From 2020, real-time geolocation tracking will supplement these investigative tools.

At the same time, investigation bodies have the authority to collect computer data from electronic communication companies.

Limitations

In order to prevent arbitrary application of any of the above-listed investigative actions, Georgian legislation sets necessary safeguards inter alia by limiting the scope, number and duration of covert investigative activities.

In terms of scope of application, Criminal Procedure Code of Georgia (hereinafter – "CPCG") limits the nature of offences which may give rise to surveillance measures and restricts categories of people that may be subject to these procedural measures.

In particular, conduction of covert investigative activities is limited to cases where an investigation has been initiated and/or criminal prosecution is conducted into intentionally serious and/or a grave offence, or several other limited types of offences listed in the Georgian Criminal Code.

Regarding the categories of people that may be subject to covert investigative activities, CPCG stipulates that in order to apply secret investigative action there must be a reasonable cause to believe that a person against whom such action is to be carried out has committed any of the offences indicated above, or a person receives or transmits information that is intended for, or is provided by, a person directly related to the offence, or a person directly related to the offence uses the communication means of the person.

It is of importance to note that CPCG requires investigative bodies to reduce the number of covert investigative actions to minimum by limiting the monitoring of communications and persons that are not related to the investigation.

As for duration, the CPCG clearly defines the maximum overall duration of covert investigative actions. Namely, it stipulates that a court warrant authorizing the conduct of a secret investigative action shall be issued for a period that is required to achieve the goal of the investigation, but for not more than one month. If this period is insufficient, the warrant may be renewed for not longer than two months upon a reasoned motion of the prosecutor, under a court ruling. At the same time, the duration may be extended one last time, for no longer than three months, upon a motion of the Chief Prosecutor of Georgia.

Another important safeguard created to prevent abuse of procedural powers is that the CPCG sets a precise list of grounds for termination of secret investigative actions, including accomplishment of a specific objective envisaged by a secret investigative action and expiry of the legal grounds for carrying out the action.

Procedures

The CPCG sets a stringent procedure to be followed for obtaining surveillance data.

To begin with, they are carried out upon a prosecutor's reasoned motion under a court ruling. In a relevant motion a prosecutor should demonstrate the standard of a reasonable cause and show a number of facts, inter alia that:

- a secret investigative action is a necessary, adequate and proportional mean for achieving legitimate goals in a democratic society and

- that information cannot be obtained through other means or it requires unreasonably great effort.

As an exception, in urgent cases it is also possible to initiate secret investigative action without a court warrant, with a prosecutor's resolution. However, in this case the prosecutor eventually has to obtain a court warrant ex post but no later than 24 hours from the time of commencing the secret investigative action. It is important to note that a covert investigative action should be terminated if urgent authorization procedure (conducted under prosecutor's resolution) is considered unlawful.

The CPCG also regulates production of computer data in general, collection of subscriber information, real-time collection of traffic data and obtaining content data.

In this regard a number of important procedural safeguards are in place. Firstly, ongoing investigation is a necessary condition to apply any of these measures. Secondly, the prosecution has to meet a specific standard of proof to obtain computer data. Particularly, there has to exist a reasonable cause to believe that information or documents essential to the criminal case are stored in a computer system or on a computer data carrier. Moreover, collection of subscriber information, traffic and content data is possible if there exists a reasonable cause to believe that a person is carrying out a criminal act through a computer system.

Above all, CPCG mandates that the prosecutor files a motion with the court, and the production of computer data is granted only on the basis of a court order. Both of these conditions constitute important safeguards against arbitrary application of the law.

Georgia also operates a system which enables direct access to communication networks, for purposes of real-time collection of traffic data and interception of content data from the service providers. Upon the request of an authorized body, an electronic communications company should give access in real time to an authorized body to the content and identification data of communications sent via its networks.

Data Management

The CPCG prescribes a set of rules to be followed for storing, using, communicating and destroying the intercepted data.

First, it establishes an important obligation of the relevant authorities to store and keep a detailed record of intercepted information and related actions. Next, it limits the persons authorized to examine the information obtained as a result of those actions to investigators, prosecutors and judges only. Furthermore, it contains detailed rules on destruction of information and materials obtained as a result of secret investigative actions.

Oversight

Georgian legislation envisages several external monitoring mechanisms of surveillance actions by law-enforcement bodies, including Parliamentary oversight and judicial oversight that has been discussed above.

In addition to these, surveillance measures are subject to the monitoring of the Personal Data Protection Inspector of Georgia. It is an independent, external supervisory mechanism authorized to ensure that law-enforcement sector complies with data protection legislation when processing citizens' personal data.

Personal Data Protection Inspector has been mandated to conduct an oversight of all covert investigative activities conducted for the crime prevention and investigation purposes.

The Inspector monitors the interception of telephone communications through an Electronic Monitoring System 24/7. Electronic Monitoring System makes it possible to observe when and on what basis is the competent authority intercepting a specific telephone communication, and when the interception ends. At the same time, the inspector receives hard copies of rulings from the court and resolutions from the prosecution (the latter in urgent cases) authorizing the interception. After comparing information received through the System and the hard copies, if any discrepancies are identified, the Inspector is authorized to suspend the interception. When these discrepancies are addressed by the relevant authority, the interception continues.

Mandate of the Inspector also extends to the monitoring of collection of computer data. Namely, a court ruling authorizing collection of computer data (or a prosecutor's resolution on the conduction of such investigative action under urgency and a subsequent court ruling finding the conducted covert investigative action lawful/unlawful) shall be submitted to Personal Data Protection Inspector of Georgia without delay. The same rule applies to the collection of subscriber information, real-time collection of traffic data and obtaining content data.

Further, the Inspector oversees access to metadata by the competent authorities. An Electronic Control System is used by the Inspector to control operations performed within the electronic communication identification databank. The system transmits the information on databank access logs and all relevant information in real time. In this regard, the law establishes an important safeguard in the form of mandatory logging by communications companies. In particular, companies record instances when the identification data of electronic communications are transferred to relevant state bodies and provide the relevant information to the Personal Data Protection Inspector. Apart from communication companies, the Inspector receives information from the court and the prosecution and compares these sources. Any inconsistences might lead to an inspection of the relevant parties.

The mandate of the Inspector extends further, after the completion of covert investigative activities. Particularly, once they are completed, the Inspector receives a protocol on the completion of the activities. In addition to this, the CPCG also lays down an obligation to destroy the information/data received from the covert investigative actions when it has no value for investigation, when it was not

used as evidence before the court, as well as after its usage, following a certain procedure. The Inspector also gets notified regarding the destruction of such information/data.

It should be noted that once the law enforcement bodies begin to use geolocation tracking from 2020, the Inspector will have the power to monitor this investigative action as well.

In addition to the above-mentioned electronic control mechanisms, the Inspector is empowered to conduct a planned or ad hoc inspection of the law-enforcement authority to check the lawfulness of data processing.

The Inspector's Office enjoys a wide range of powers during inspections. It is authorized to request any document and information on any issue regarding data processing, including classified information. The Inspector and authorized personnel are entitled to enter the areas of limited access and monitor data processing on site.

The Inspector is also equipped with efficient tools for enforcement of data protection legislation – including issuing mandatory instructions and imposing fines. If a data controller fails to comply with the instructions, the Inspector is entitled to address the court. If during the supervision process the Inspector identifies any sign of a criminal conduct, he/she informs relevant investigative authorities.

It is important to note that the Inspector is accountable to the Parliament of Georgia to which he/she presents an annual report. Annual reporting also includes providing information on the results of monitoring of surveillance.