Institute for Development
of Freedom of Information

Risks and Challenges of the Draft Amendments to the Law of Georgia on Information Security

November, 2019

Introdution

Institute for Development of Freedom of Information (IDFI) responds to the Draft Amendments to the Law of Georgia on Information Security initiated to the Parliament of Georgia on October 2nd, 2019.

The rapid development of information technologies increases the dependence of every member of society on modern electronic systems. At the same time public services, structures and security systems are increasingly dependent on constantly updating digital technologies. These developments pose both internal as well as external risks. Identifying such risks and implementing relevant measures of protection are crucial in the given reality. However, it should also be taken into account that Georgia is a young democracy, with developing systems of good governance and accountability, thus potential unsubstantiated increase of the state control over information security should not be implemented at the expense of restricting human rights and freedoms.

The existing Law of Georgia on Information Security is based on the principles of coordination and cooperation between the private and the public sectors, while the new draft amendments to the law aim to impose stricter regulations in the area of information security by coordinating it under the Operative-Technical Agency (OTA) of the State Security Service of Georgia. The new regulations would be applicable to state institutions as well as private organizations. This could be considered as a major reform in the area of cybersecurity.

IDFI finds that the new draft law, initiated to the Parliament of Georgia on October 2nd, 2019 poses a number of significant threats discussed below.

1. Major Reform of the Information Security System

According to the current regulations and the Cyber Security Strategy of Georgia 2016-2018, approved by the decree of the Government of Georgia, the set-up of the cybersecurity system is as follows:

In 2010 Data Exchange Agency (DEA) – LEPL of the Ministry of Justice (MoJ) was established. DEA is mandated to protect critical information systems and introduce information security standards.

The agency also monitors the entire governmental networks and conducts audits of state information systems. The Computer Emergency Response Team operates under the umbrella of DEA, which is responsible to detect and suppress cyber incidents.

In December 2012 Special Cybercrime Unit was ceated within the Central Criminal Police Department of the Ministry of Internal Affairs of Georgia (MIA), which investigates cybercrimes throughout the country. The unit also constitutes an international contact point with the mandate related to international law enforcement coordination in accordance with the CoE Convention on Cybercrime.

In 2014 LEPL Cybersecurity Bureau (the Bureau) was established within the system of the Ministry of Defense (MoD) in order to ensure cybersecurity in the defense sector. The Bureau was tasked to suppress and prevent cyber-attacks directed against the critical military infrastructure of Georgia.

In order to effectively execute its mandate, the Bureau analysis defense sector infrastructure and ensures implementation and further development of information security mechanisms.

In 2014 the State Security and Crisis Management Council (the Council) of Georgia was established under the Prime Minister of Georgia. Prior to its abolishment the Council was responsible for developing the overall framework of cybersecurity policy in the country. At the same time, the Council had the obligation to take relevant measures to tackle critical incidents of cybersecurity at the national level.

The State Security Service of Georgia is responsible to detect, suppress and prevent the activities in cyberspace directed against the **national security** of Georgia. By virtue of law, the State Security Service also constitutes an agency with the exclusive authority to conduct covert investigative activities in cyberspace.

The proposed version of the draft law fundamentally changes the current cybersecurity architecture. LEPL Operational-Technical Agency (OTA) of the State Security Service is, in fact, becoming the main coordinating and supervisory body of information and cybersecurity. The mandate of the Agency covers the critical infrastructure of public as well as private entities. The draft law does not clearly indicate the mechanisms through which interagency coordination will be strengthened. Quite on the contrary, according to the draft law the governance pillar of cybersecurity is added by another agency authorized to supervise relevant institutions, and at the same time cooperate with them (including via issuance of joint orders). This will further complicate cybersecurity management process. Regarding the process of coordination, the draft law does not precisely provide roles and functions of the relevant structural divisions of MoD and MIA.

According to the draft law, DEA (LEPL of MoJ) is responsible to exercise its power in coordination with OTA (LEPL of the State Security Service). Pursuant to the draft law, the Computer Emergency Response Team of DEA implements the following activities in close coordination with OTA: a) public educational campaigns on the topic of information security; b) Warning the wider public and disseminating information on forthcoming threats; c) Representing the country on the international level in regards with information security; and d) Rising public awareness on the issues of information security (article 8^1 of the Draft Law). According to article 6(2), objects of critical information infrastructure falling under tier 2 or 3 are obliged to submit audit reports prepared by DEA or other entities authorized by DEA, to OTA **on a mandatory basis.**

Despite the fact that these two agencies will issue orders and other bylaws regulating information security, under the new arrangements, DEA will cease to have supervisory mandate and it will be transferred to OTA. For instance, the objects of critical information infrastructure falling under tier 1 and 2 should submit their annual reports to the OTA whereas only the objects falling under tier 3 will be accountable to DEA. At the same time, DEA will be in charge to monitor the standards of information security within the private sector only through close cooperation and coordination with

OTA. **Thus, under the given circumstances the mandate of DEA Computer Emergency Response Team is vague.**

It should be highlighted that the substantive reform in the area of information and cybersecurity is being implemented under the circumstances when GoG still has not approved a new Cybersecurity Strategy and Action Plan. The draft law was prepared and initiated by the MP – Mr. Irakli Sesiashvili. AoG was neither the initiator nor the author of the draft law. It is also unclear to what extent the newly created National Security Council, the predecessor of which elaborated the framework of the national cybersecurity policy was involved in the process of preparing the draft law. In addition, there is no information on the extent to which the draft law was discussed and agreed with those private sector representatives, which will be directly affected by the new stricter regulations (that will highly probably be adopted in the nearest future).

2. Problems of Grouping the Subjects of Critical Information Infrastructure into Tiers and High Risks of Unjustified Interference into the Protected Area of Human Rights

According to the explanatory note of the draft law, the main aim of the amendments is to introduce a new system of categorization for the objects of critical information infrastructure and introduce new oversight and administrative liability mechanisms applicable to them.

The draft amendments introduce the following three-tear categorization for the objects of critical information infrastructure (three tears):

a) **Tier 1** – state agencies, institutions, LEPLs (other than religious organizations) and state enterprises;

b) **Tier 2** – electronic communication companies;

c) **Tier 3** – banks, financial institutions and other entities of private law.

Together with introducing general obligations for the objects of critical information infrastructure (e.g. appointing information security officers and conducting mandatory audits), the draft law also sets various regulations in terms of their control and administrative liability.

The most challenging regulations are applicable to the objects of critical information infrastructure falling under tier 1. Namely, they will have the obligations to:

a) Establish network sensors and ensure access of OTA to them;

b) Ensure that upon the request of OTA, the agency has immediate access to their information assets, information systems and/or their integral parts when the access is necessary for responding to cyberattacks or their prevention;

c) Accept scheduled or random mandatory inspections of their respective information and telecommunication infrastructures;

d) Implement necessary measures included in the audit reports and be the subjects of administrative responsibility in case if they fail to do so.

According to the GoG Decree on the Approval of the List of Critical Information Infrastructure Objects adopted on April 29th, 2014, various public institutions, including those not falling under the authority of GoG are grouped under tier 1, e.g. such institutions are: the Parliament of Georgia, the Administration of the President, Tbilisi City Hall, Central Election Committee, the National Bank of Georgia, JSC Georgian Railway, LLC Georgian Aero Navigation, etc. **Therefore, proposed amendments will enable OTA to have access to the information infrastructure, systems and assets of the objects of critical information infrastructure falling under tier 1. Moreover, by virtue of Article 10(4) of the draft law, OTA will be granted the authority to manage the sensors and monitors installed at these institutions in order to identify relevant cyber-attacks.**

Georgian legislation sets the broad definition of **information assets** and covers any knowledge or information important for the objects of critical information infrastructure, namely, technological means for storing, processing or transmitting information and their knowledge on processing data. Objects of critical information infrastructure conduct assessment of their information systems and ensure the categorization of each information asset as – '**confidential'** or **'for internal use only'.**

Although the current version of the Law on Information Security envisages the applicability of the above-mentioned legal notions, the General Administrative Code of Georgia does not include the definition of 'confidential information' or 'information for internal use only'.

The General Administrative Code of Georgia exhaustively provides grounds for denying access to public information, namely the information including state, commercial or professional secrets or personal data.

Hence, there is an inconsistency between the Law on Information Security and the General Administrative Code of Georgia. As a result, the classification of information as 'confidential' or 'for internal use only' is not clear. At the same time, such broad interpretation of the above-mentioned categories of the restricted information provided by the current version of the Law on Information Security increases risks of arbitrary interference and unjustified restriction of access to public information.

Based on the ordinance of DEA of February 4th, 2013 on Approving the Rules of Network Sensor Configuration a network sensor implies installation of a software on a computer server that enables storing of information on the state of and connections between networks/segments of networks and sending information to the central collection server via secure channels stationed at DEA. According to the ordinance the following information is sent to the Central Collection Server: a) incoming and

outgoing connection destinations – specific IP addresses; b) connection establishment and termination date etc. **However, it should be emphasized that modern information and communication technologies can be configured in a way that enables collecting relatively vast categories of data including real-time monitoring of the content.**

The abovementioned factors increase the risk of State Security Service of Georgia gaining unlimited access to information on indefinite number of individuals with the help of modern technologies. Even though there is a presumption that the respective authority will not abuse its power by means of these technologies, the mere technical possibility of the agency to access, obtain and manage personal data in real-time and to process data enabling identification of specific individuals (metadata) creates risks for unjustified interference into the protected scope of private life. The constitutional court of Georgia found that there was a similar risk of unjustified interference into the protected scope of private life, when it set restrictions for State Security Service of Georgia to have unlimited access technical means of surveillance.

In the process of categorizing objects of critical information infrastructure, significant problems were identified related to the objects falling under tier 2 and tier 3, which mainly cover representatives of the private sector. The most problematic aspect in that regard is the extent of tier 2, covering private electronic communication companies (as defined by the Law on Electronic Communications) according to Article 1(G²) of the proposed draft law.

In this case, the approach based on which the companies are grouped under tier 1 and tier 2 is ambiguous. It is also unclear why electronic communication companies are subject to a higher standard of accountability towards OTA. According to Article 4(3) of the draft law, objects of critical information infrastructure falling under tier 2 - telecommunication companies, will be obliged to submit internal regulations on information security and any amendments made to them to OTA. The same rules apply to the objects falling under tier 3, which shall submit the information to DEA.

OTA Computer Emergency Response Team is entitled to direct electronic communication companies to take necessary measures to identify and neutralize computer incidents in its infrastructure in order to prevent their reoccurrence in the future. It should be noted that the failure to do so entails administrative responsibility, which might render objects falling under tier 2 more vulnerable to OTA, as they would be more likely to grant OTA access to their infrastructure, including network sensors in order to avoid fines.

The most problematic aspect in the process of categorizing objects of critical information infrastructure falling under the regulations of the new draft law is that the categorization will be conducted based on a government decree (Article 2(1) of the draft amendments). Thus GoG will be entitled to determine which organizations should be subject to stricter or lighter regulations, without conducting any prior consultations with relevant stakeholders.

3. Standards of GoG Decree Regarding the Receipt and Processing of Personal Data by the Objects of Critical Information Infrastructure

The provisions of Article 82(1) of the draft law, according to which GoG decree will determine requirements for manufacturers developing hardware and software used in the process of receiving, processing, storing and transmitting personal data by the objects falling under tier 1 and tier 3, is also problematic. By virtue of this article, GoG will have the authority to set certain restrictions for private companies purchasing, upgrading or using their respective IT systems. The noncompliance with these requirements will result in imposing administrative fines of up to 5 000 GEL. Such an approach per se is contradictory to the core principles of the free market and fair competition.

Taking into consideration existing challenges of cybersecurity in Georgia there is a pressing need to amending the Law of Georgia on Information Security, particularly in regards to its enforcement mechanisms. However, based on the risks and threats identified by IDFI we call on the Parliament of Georgia to:

1. Turn down the draft amendments to the Law of Georgia on Information Security;
2. Start reforming the Cybersecurity System of Georgia only after the National Cybersecurity Strategy and Action Plan are adopted;
3. Ensure the active participation of all relevant stakeholders, including the representatives of local and international organizations as well as the private sector in the process of preparing draft amendments to the Law of Georgia on Information Security.