Project Cybercrime@EAP III
Public/private cooperation

Արևելյան Գործընկերություն
Східне партнерство Eastern
Partnership აღმოსავლეთ
პარტნიორობა Parteneriatul
Estic Şərq tərəfdaşlığı Partenariat
Oriental Усходняе Партнёрства

2017/DGI/JP/3608
19 April 2017

REPORT ON GEORGIA

Prepared by the Cybercrime Programme Office with input from the member of the Cybercrime Convention Committee (T-CY) Bureau Markko Künnapu and Council of Europe's expert Marko Jurić

ON

Draft legislation supplementing and amending various issues related to cybercrime and electronic evidence

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to represent the official opinion of the European Union.

The views expressed in this document are of preliminary nature pending additional clarifications and do not, in any way, represent the official view of the Council of Europe and its institutions.

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

BACKGROUND INFORMATION

The request for review originated from the discussions within the framework of activities under the Cybercrime@EAP II and Cybercrime@EAP III projects implemented by the Cybercrime Programme Office of the Council of Europe. The country team of these projects informed the C-PROC staff and experts present at various seminars and workshops throughout 2016 that there are plans to prepare amendments aimed to bring the criminal procedure law of Georgia in closer compliance with the Budapest Convention on Cybercrime.

The package of amendments (English translation appended to this summary) is currently being developed by the working group comprising of various state agencies, and was shared preliminarily with the Council of Europe Cybercrime Programme Office for unofficial and informal consultations on the issue of compliance with the Budapest Convention.

The meetings on the issue with the country team/working group of draft authors were held in Tbilisi on 16-17 February 2017.

During the meeting the text of amendments as well as reasons that triggered the reform were discussed. It was also mentioned by Georgian authorities that several other amendments related to production order as well as search and seizure were being prepared.

Bearing in mind the observations and recommendations given below, we encourage the Georgian authorities to continue with the legal reform.

However, in order to solve all the practical problems related to computer data and electronic evidence, all the amendments that are related to the subject should be merged into one legislative package. The experts fully understand the concern not to lower existing conditions and safeguards prescribed by the national law, but we also advise the drafters to avoid going too much farther, because it might in turn have overall negative impact of the speed and effectiveness of the investigations.

As the proposed amendments would have direct effect on the work of the law enforcement authorities and judiciary we would like to stress that all stakeholders should be consulted.

I. PRELIMINARY OVERVIEW OF AMENDMENTS

1. Definitions

a. The amendments refer to the new definitions of subscriber information, current implementation of which is deleted from existing version of Article 136 and has been moved to the list of definitions under the Law on Electronic Communications (term "user identification data" under par. z^{72} of Article 2 of the Law). The concept of "identification data of communication equipment" is introduced in the next paragraph of the same Law, for seemingly no particular reason as there is hardly any difference in treatment of this data from the procedural law perspective as compared to subscriber information (ref. below to discussion on production orders under par. 1-3 of Article 136 CPC). It needs to be determined whether both of these proposed concepts, which now include a much broader scope than current version of the definition of subscriber information, correspond to the Convention language, bearing in mind not only the need to define subscriber information broadly[1] but also the differences related to traffic data.

b. In terms of definitions under Article 3 of the Georgian CPC, the revised draft introduces slightly revised concept of service provider, new concept of storage device, and refers to new definitions of subscriber/device data; however, in doing so, it seems to replace the current wording of par. 30 of Article 3 which is/was an implementation of the traffic data definition (perhaps a numbering mistake or omission). Amendments also introduce the definition of storage device. The need for this particular definition might require additional explanation.

[1] Please refer to, e.g., Guidance Note on Subscriber Information, https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)26_guidanceNote8_subscriber%20info_V10.pdf

Ideally, the law should be as technology neutral as possible. Therefore, it should be further analysed whether this new definition is needed.

c. It is important to have a close review and comparison of all the newly introduced definitions, because definitions related to user identification data and equipment data might overlap. Very often data which might identify the user – IP address, phone number etc. is considered as part of subscriber information i.e. user identification data.

2. Data preservation

First and foremost, the amendments aim to address the issue of the preservation of data implementing the Article 16 of the Convention, which was previously absent from the Georgian legislation. In this regard, new wording of Article 137 is introduced into the Criminal Procedure Code of Georgia, which is a welcome development to address the issue of preservation, which is not purely a national exercise but also has direct effect on international cooperation, especially through the 24/7 points of contact under the Budapest Convention.

Normally, the preservation of data should happen as quickly as possible and usually this is the power that is reserved for investigators to be applied, while the draft requires the prosecutor's decree. However, taking into account the nature of the criminal procedure of Georgia, in which prosecutors are almost immediately involved with investigation and provide it with full guidance, the proposed prosecutorial power is acceptable from the perspective of expediency.

At the same time, it would be advisable if the implementation of Article 16 is also followed by discussion on the role of the prosecutors in the process of cooperation between 24/7 points of contact. Data preservation is one of the most frequent requests being processed by 24/7 network and urgent interaction with prosecutors is thus essential to make the proposed provision work in the international cooperation context.

The only question that it is left unclear is whether the amendment causes deletion of the existing wording of current Article 137 of the CPC, which was implementing Article 20 of the Convention (real-time collection of traffic data). Discussions with the country team on this subject would still be necessary.

3. Production orders

Amendments are being introduced to the current wording of Article 136 of the Georgian CPC, which currently implements the provisions of Article 18 of the Budapest Convention (production order). It is fair to say that this provision has been revised entirely, which should be somewhat surprising, given that the previous assessments of Georgia indicated that the current implementation of Article 18 by Article 136, with one reservation, is generally complaint with the Convention.[2]

Irrespective of this, there are several aspects to this provision that can be cause of concern:

a. The draft splits the current procedure of production under par. 1 of Article 136 of the CPC, based on judicial order, into two separate paragraphs (1 and 2) of the same Article. The differences therein can be summarized as follows:

    i. Par. 1 refers to "electronic communications content data" as opposed to "data identifying electronic communication" in par. 2 (perhaps, to differentiate production of content data vs. subscriber information?). It should also be noted that electronic communications content data as such is quite limited and excludes many other types of data;
    ii. Par. 1 refers to storage/maintenance of data by service provider, while par. 2 also adds the reference to data stored by the central data bank of the State Security Service (i.e. mass retained data);

    which seems to: 1) defeat the purpose of such division rather than purely theoretical exercise, as the judicial order is required in both of these instances, and, 2) if references to subscriber information and content data are assumed to be made, this brings the question of treatment of the traffic data which seems to be absent from these provisions.

[2] Please refer to the EAP Cybercrime Legislation report from 2012, embedded at the end of the file.

b. Par. 3 of Article 136 presumably aims to lower the standard for issuance of production orders with regard to subscriber information, by deleting the need for judicial authorization in cases where there is "reasonable cause to believe that a person is carrying out a criminal act through a computer system or information essential to the criminal case is stored in a computer system". If this is done to differentiate this procedure from the judicial order-driven procedures under par. 1 and 2 of the same Article, the question is whether reference made to "identification data of a user and/or identification data of communication equipment" in par 3 is any different from the concept of "data identifying electronic communication" in par. 2 (and, also, its difference from the "electronic communications content data" in par. 1) of the same Article.

4. Safeguards and guarantees (Article 15 of the Convention)

With regard to the proposed conditions and safeguards, the first impression is that they are stipulated in very detailed manner and compared to the rest of the CPC might go too far. Bearing in mind the possible technical mistakes of wrong numbering as there are two paragraphs 3 of Article 136, the par. 3 to 14 of the same Article are meant to enforce safeguards and guarantees in relation to production order procedures, perhaps in order to address the implementation of Article 15 of the Cybercrime Convention:

a. The question of scope is instrumental as it seems that these detailed regulations concern only a production order. As such, any investigative measure sourced from the Budapest Convention may constitute interference with right to private life and privacy, but such interference might not be so severe to justify all of these conditions. To put this into perspective of other investigative powers, it seems that currently the threshold might go even higher for production order than orders for interception of communications; or, if this is the standard, then it must be also asked if the same safeguards and guarantees need to be applicable not only to the production orders, but to more intrusive provisions of monitoring of traffic data and interception of content, currently addressed by Articles 137 and 138 of the CPC. If all those conditions need to be fulfilled only with regard to production order, then threshold goes too high and criminal justice system is out of necessary balance as required by Article 15 of the Cybercrime Convention.

b. Additionally, these safeguards are applicable only to par. 1 and 2 of the same Article, meaning the production orders on the basis of the judicial decisions, and do not relate to provisions of par. 3 which authorize streamlined production of data without judicial decision.

c. Draft law introduces a requirement that production order may be used only if imprisonment sentence is possible. This might go too far and might be in conflict with the Convention. In addition it might cause problems for international cooperation if Georgian competent authorities receive request to produce data from other country.

d. The language used in these provisions is very broad and general in nature, and perhaps a few questions need to be asked to the authors if there are specific procedures to put these guarantees into action. For example, it seems that regulation proposed in Article 136, par. 5-8 is out of place, as proportionality and necessity are principles that apply to entire criminal proceedings and should be taken into account while conducting any procedural measure. Moreover, it creates an additional obligation and workload for the law enforcement/judicial authorities, because in order to continue with the production order they need to assess whether all the criteria has been fulfilled. Otherwise the measure could be very easily declared invalid if appealed.

e. Authors of the draft law should analyse further whether special appeal mechanism (Art 136, par. 9-10) is needed here. Normally there are general rules that enable a person to challenge or appeal any measure that has been carried out. Having special procedure only for production order is not logical. It makes also the work of the law enforcement/judicial authorities more difficult, because there could be appeals that are based on different legal grounds.

f. The revised draft contains reference to several provisions from the Chapter XVI[1] of the Georgian CPC regulating the conduct of secret investigative actions. While some numbering again seems to be wrong, these refer mostly to similar safeguards and guarantees applicable in case of covert application of the procedure – in this case, the production order. However, question need to be asked as to in which cases covert production is envisaged to be performed,

as the production of document or data is in itself an overt procedure that may be simply subject to requirement of confidentiality? Also, production of data seems to be entirely absent from an authorized list of covert investigative measures provided in Article 143[1] of the CPC and thus would not be – in theory - authorized.

II. SUMMARY OF THE DISCUSSIONS HELD DURING THE MEETING WITH GEORGIAN AUTHORITIES IN TBILISI ON FEBRUARY 16-17 2017

Roundtable on legislative amendments took place in Tbilisi Georgia on 16-17 February. From Georgian side representatives from the Office of the Chief Prosecutor and State Security Service attended the roundtable.

Discussion focused on proposed amendments to the Criminal Procedure Code of Georgia, in particular Articles 136 and 137 as well as preliminary findings of the Report on Georgia from 3 February 2017.

Georgian authorities gave an introduction to the amendments proposed and explained their background. As the existing Article 136 of the Criminal Procedure Code was limited and as Georgian courts had started to interpret the legislation in a restricted manner concerning its scope and conditions and safeguards, amendments were proposed. Special attention was paid to recent judgment of the Constitutional Court of Georgia.

The main purpose of the amendments was to provide for clear rules on requesting computer data from service providers. Although amendments would replace existing regulation the purpose at the same time is not to lower existing conditions and safeguards.

As Georgian legislation on procedural measures of the Budapest Convention is not fully in line with the Convention, discussion focused also on how to improve Georgian legislation in order to implement the Convention standards to full extent.

While discussing measures addressing computer data and electronic evidence, it was also mentioned by the Georgian authorities that other amendments were being prepared in parallel, in particular on search and seizure and international production order.

Although the experts understood the practical problems that had been emerged and the need for legislative amendments related to law enforcement authorities' access to computer data, certain concerns were expressed in particular with regard to the scope of the proposed regulation, thresholds, conditions and safeguards and specific rules on appeals and immunities.

III. RECOMMENDATIONS TO THE ONGOING LEGISLATIVE PROCESS AND DRAFT AMENDMENTS

Based on the proposed amendments and discussion that took place during the Roundtable in Tbilisi on 16-17 February, experts would like to present the following observations and recommendations.

1. As there are several draft laws related to access to computer data they should be merged into one draft law or package. Draft laws on criminal procedure measures related to computer data and electronic evidence (production order, international production order and search and seizure) due to their close relation to each other, should be analysed together and consulted with all the relevant stakeholders.

2. When drafting new definitions, the definitions from the Budapest Convention, i.e. on subscriber information, traffic data etc., could be considered as guidance.

3. Production order as provided by the Budapest Convention (Article 18) should cover any natural or legal person possessing or having under its control any computer data. This includes, but is not limited, to service providers. As a preliminary point, it should be emphasized that current Article 136 of the Criminal Procedure Code follows the text and purpose of Article 18 of the Convention. On the other hand, new Article 136 of the Criminal Procedure Code as proposed, narrows the scope of the production order only to service providers.

4. We suggest not to narrow the scope as proposed, because it would leave out several categories of persons. Alternatively, the law could provide a general and special provisions on production order. As Georgian legislation currently has specific provision on production order in place then using search and seizure in the future to obtain data from person not being service provider, is a huge step backwards. Although using search and seizure to give effect to Article 18 might be valid under the Convention, such solution is not preferable, both in terms of the Convention and Georgia's national law. In this context, it is also necessary to consider Article 6(3) of the Criminal Procedure Code, which stipulates that "preference shall always be given to the less severe form of restriction of rights and freedoms". Unfortunately, such preference cannot be given if relevant authorities do not have less severe measure at their disposal.

5. As production order is to be considered as open measure contrary to the special investigation measure, reference to the Law on Operative- Investigative Activities should be left out. Production order as measure should be applicable in any criminal investigation and not to be restricted to serious crime only. That would enable Georgian authorities to execute requests from other countries and fulfill the obligations derived from international treaties including the Budapest Convention.

6. In Nadia Khurtsidze and Dimitri Lomidze v. The Parliament of Georgia, the Constitutional Court ruled that current Article 136 is unconstitutional, to the extent that it prevents defense in criminal proceedings from obtaining computer data. As a preliminary point, we believe that this issue falls outside the scope of the Cybercrime Convention, since it concerns general principles of criminal proceedings. Nevertheless, we are of the opinion that consequences of the ruling could be addressed in the amendments to the CPC.

7. Article on the production order could foresee different conditions and safeguards which would depend on the categories of data. Proposed Article 136 introduces differentiation between three categories of data, namely electronic communication content data, "data identifying electronic communication" and "identification data of a user and/or identification data of communication equipment". Different conditions and safeguards are envisaged. Experts are of the opinion that these conditions and safeguards should be reviewed, in the light of the following observations:

    a. Differentiation between first two sets of data (paragraphs 1 and 2 of the proposed Article 136), which would require court order, and the third (paragraph 3), which could be produced on the basis of prosecutor's or investigator's order, is considered acceptable.

    b. Conditions and safeguards envisaged in paragraph 5 of the proposed Article 136 should be removed. The main problem here is that the application of this provision could in practice lower the standard of human rights protection. The reason for this is that legitimate goals for the application of Article 136 mentioned therein go beyond the scope of criminal procedural law. Therefore, application of Article 136 is *de facto* broadened beyond, to include situations which should not fall within the scope of the Criminal Procedure Code.

    c. Moreover, paragraphs 5, 6, 7 and 8 of the proposed Article 136 seek to introduce different requirements which can be considered as parts of necessity / proportionality test. In experts' opinion, paragraph 5 is superfluous since requirement to pursue legitimate goals is already achieved. This is because Criminal Procedure Code as a whole contributes to prevention and sanctioning of crime. Moreover, requirement of necessity is already present, explicitly or implicitly, in other CPC's provisions (i.e. that data is "essential to the criminal case", Article 136(1-3), or Article 6(3) which mandates that less severe restrictions are applied), or as a requirement arising under the Constitution, ECHR or Cybercrime Convention.

    d. For similar reasons, paragraph 6 is superfluous since it can be presumed that measures undertaken on the basis of the Criminal Procedure Code are carried out due to some pressing social need. Moreover, where computer data are needed, it can hardly be disputed that production order is adequate and proportionate method of gaining access to those data.

e. In relation to paragraphs 7 and 8, where computer data are needed, production order is the least intrusive method of obtaining it (other than voluntarily submission by the data holder). As explained above, alternative to production order is search and seizure, which is by definition more intrusive procedural power.

8. To conclude, experts recognize that these provisions are modelled upon requirements mentioned in Article 8(2) of the ECHR. However, experts are not convinced that these provisions should be introduced in the Criminal Procedure Code in the present form, since the requirements arising under ECHR are properly introduced in national law by making appropriate and more specific legislative choices. In any case, even if these safeguards are to be introduced explicitly in the Criminal Procedure Code, due to their general and horizontal nature they should be moved to the General Part of it.

9. Special appeal procedure proposed in the Article 136 should be left out. If necessary existing rules on appealing against the action or decision on application of procedural measure (CPC Article 95 etc) should be amended. Having both general rules on appeals and special rules for production order would reduce legal clarity. Parallel appeal procedures might also hinder the effectiveness of the investigation.

10. Special rules on persons enjoying immunity or having special status (Members of the Parliament, judges etc) should be left out, because initiating criminal investigation and permission to carry out procedural measures is covered by general rules (CPC Article 143[3] (17), Article 167 (5).

11. If existing provision couldn't be used to request data from foreign service providers, special provision might be of help.[3]

12. Computer data that has been lawfully collected or obtained by the government institutions and processed in governmental databases shouldn't be subject to a production order. Alternatively a special provision could be foreseen that would regulate law enforcement authorities' access and obtaining data from there.

13. Rules on search and seizure, with a special focus on computer systems and computer data should be reviewed in order to make them in line with the Budapest Convention (Article 19).

14. Rules on examination of the computer system, storage device or computer data should be reviewed. If computer system or storage device has been lawfully seized, we don't see the need for requirement for an additional court order to examine the content.

15. As a general principle, necessity to access and use computer data by law enforcement authorities should not be verified by personal data protection authorities. In particular, any restrictions of the right to personal data protection within the criminal proceedings should properly be addressed and decided by relevant law enforcement authorities and the courts. On the other hand, personal data protection authorities can have role in ensuring that storage and /or retention of data are done in accordance with personal data processing principles.

IV. OTHER ISSUES

a. Data retention

Major part of the current discussions in Georgia with regard to electronic evidence and law enforcement action in cyberspace relates to reform of the data retention system, which was found to be unconstitutional by the decision of the Constitutional Court of Georgia in 2016, on the grounds of proportionality (storage for 2 years) and lack of impartiality (storage by State Security Service). As the Cybercrime Convention does not regulate the issue of data retention, these discussions would be outside the scope of the action requested from the Cybercrime Programme Office and thus no respective drafts were shared with C-PROC for review.

[3] With understanding that some or all of these issues would be resolved once provisions on international production order are introduced.

At the same time, it would be advisable to take into account the current system of data retention – to be reformed by March 2017 – which is contained in the Article 8^3 of the Law on Electronic Communications, since data retention is an important prerequisite for legitimate creation of stored data that can be later accessed to and used by the law enforcement as electronic evidence in criminal investigations.

Discussion with the country team on this subject, bearing in mind the limited scope of the mission, would still be necessary.

b. More opportunities for reform

Beyond addressing the provisions of Articles 16 and 18 of the Cybercrime Convention, the Georgian authorities seem to be missing an opportunity to complete the reform of the criminal procedure to achieve even closer – if not full – compliance with the Budapest Convention. Notable opportunities for further reform include:

- Lack of implementation of the Article 17 of the Convention on expedited preservation and partial disclosure of traffic data;

- Lack of implementation of specific powers related to computer search and seizure, such as par. 2 (extension of search) and par. 3 (retaining copies of computer data and rendering data inaccessible) of Article 19 of the Convention;

- Lack of review of provisions related to real-time monitoring of traffic data (Art. 20 of the Convention) in terms of applicability of different standards and safeguards with regard to less privacy-intrusive nature of such monitoring, which would reinforce the importance of having a higher standard applicable to interception of content (Art. 21 of the Convention).

Convention language	Current law of Georgia	Proposed amendments
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and		

ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21		
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights,	Privacy of individuals is ensured by the Constitution of Georgia and other relevant Acts. **Constitution of Georgia** **Article 20** 1. Everyone's private life, place of personal activity, personal records, correspondence, communication by telephone or other technical means, as well as messages received through technical means shall be inviolable. Restriction of the aforementioned rights shall be permissible by a court decision or also without such decision in the case of the urgent necessity provided for by law. 2. No one shall have the right to enter the house and other possessions against the will of possessors, or conduct search unless there is a court decision or the urgent necessity provided for by law. **Criminal Procedure Code** **Chapter II. Principles of Criminal Procedure** **Article 6. Impermissibility of Unlawful Restriction of a Person's Constitutional Rights and Freedoms** 1. The restriction of a person's constitutional rights and freedoms shall be permitted only on the basis of the	

responsibilities and legitimate interests of third parties.	special provisions provided by the Constitution and this Code. 2. Passing a verdict of a guilty and imposition of a sentence thereon shall be the exclusive authority of the court. 3. Preference shall always be given to the less severe form of restriction of rights and freedoms. **Article 7. Inviolability of Private life** 1. A party is not authorized to interfere wilfully and unlawfully in the private life of another during the investigation. The law guarantees inviolability of a private or other property and private communication through any means. 2. A person responsible for a procedural action shall not disclose data related to individual's private life, as well as information of private character, the confidentiality of which a person deems to be necessary. 3. A person who has suffered from an unlawful disclosure of data regarding his/her private life shall be entitled to fully recover the damages in accordance with the procedure established legislation of Georgia. **Law of Georgia on Electronic Communications** **Article 8 - Maintenance of the confidentiality of information in the field of electronic communications** 1. Information on a user of electronic communication networks, also information transferred by a user via said networks, shall be confidential and its confidentiality shall be guaranteed by the legislation of Ge orgia. 2. All persons employed in the field of electronic communications are obliged to maintain the confidentiality	

	of information referred to in paragraph 1 of this article. Employees and other persons working in the field of electronic communications shall be held liable in accordance with the legislation of Georgia if they reveal such information. 3. The obligation of confidentiality of information provided for in paragraph 1 of this article shall not apply to cases where an authorised body carries out covert investigative activities envisaged by Article 143 [1](1) (a, b) of the Criminal Procedure Code of Georgia. 4. A person employed in the field of electronic communications shall, in accordance with the procedure determined by Chapter XVI[1] of the Criminal Procedure Code of Georgia, transfer the data provided for in paragraph 3 of this article to the body carrying out covert investigative activities, in accordance with the procedures established by the Law of Georgia on Intelligence Activities and the Law of Georgia on Counter Intelligence Activities, respectively, to the body carrying out intelligence or counter intelligence activities, and in accordance with the procedure specified in Article 7(3) of the Law of Georgia on Special Investigative Activities, to a body conducting special investigative activities, in the following cases: search for a missing person; search for an accused or convicted person in order to present him/her to the relevant state body if he/she avoids the application of imposed coercive measures or service of the imposed sentence; se arch for property lost as a result of a crime. 5. Information on the content of the communication made by a user via an electronic communication network shall be immediately and automatically destroyed. Said information may become available only to the entity specified in Article 8[1] of this Law in accordance with the procedure established by law	

	Law of Georgia on Operative-Investigative Activities **Article 5 - Publicity and operative-investigative activities** 1. Operative-investigative activities are highly classified. The data, documents and sources relating to such activities shall be made available for inspection in a prescribed manner only to the persons specified in this Law, and to the Data Protection Inspector and a person designated by him/her, within the limits envisaged by the Law of Georgia on Perso nal Data Protection. 1^1. A prosecutor may, by a reasoned order, declassify documents and materials relating to operative-investigative activities (except for the documents and materials specified in Article 21(2) of this Law) in order to use them as evidence, unless the declassification of such documents and materials prejudices the vital interests of the country in respect of d efence, economy, foreign relations, intelligence activities, state security and public order. 2. The disclosure of information on operative-investigative activities by a person to whom such information has been confided or who has become aware of such information in connection with his/her offici al duties, shall incur criminal liability for disclosing a state secret. 3. (Deleted - 1.8.2014, No 2635). 4. Information on a secret collaborator engaged in operative-investigative activities or the source of information may not be revealed or disclosed irrespective of the elapsed time, except as provided for by this Law. 5. (Deleted - 1.8.2014, No 2635).	

	Article 6 - Legal guarantees for protecting human rights and freedoms, as well as the rights of legal persons in operative-investigative activities 1. Operative- investigative activities may not be carried out in pursuanc e of objectives that are not provided for in this Law. 2. A person who considers that an operative-investigative measure conducted with respect to him/her has resulted in an unlawful restriction of his/her rights and freedoms may appeal against the lawfulness of such an operative-investigative measure to a higher state authority, prosecutor or court. If such operative-investigative measures are recognised as unlawful, the information obtained by such measures shall be deemed inadmissible evidence in accordance with the Criminal Procedure Code of Georgia. The burden of proving the lawfulness of an operative-investigative measure shall be with the authority that conducted the operative- investigative measure. 3. Authorities (public servants) conducting operative-investigative activities shall be prohibited from secretly participating in the activities of the legislative, executive and judiciary bodies, or in the activities of the supreme representative bodies of the Autonomous Republics of Abkhazia and Adjara and of local self-government bodies. It shall be prohibited to secretly participate in the activities of officially registered public and political organisations or religious organisations, unless such activities are intended to subvert or forcibly change the constitutional order of Georgia, to encroach on the independence of the country, to violate the territorial integrity of Georgia or unless such organisations are engaged in war propaganda or violence, or incite national, local, religious or social discord. In those c	

	ases, the consent of the Chief Prosecutor of Georgia is req uired. 4. Information that has been obtained by operative-investigative activities and that is not related to a person's criminal activities, but contains details of his/her private life, may not be disclosed or used for any purpose. Such information may not be stored and it must be immediately destroyed. The destruction of such information shall be notified to the Chief Prosecutor of Georgia and the court in the territory where the operative-investigative measure has been conducted or the court according to the place of investigation. 4^1. The materials obtained through an operative-investigative measure specified in Article 7(3) of this Law shall be destroyed upon the lapse of 6 months after the termination of the operative-investigative measure. Such materials shall be destroyed by the prosecutor who filed a motion with the court for the conduct of the operative-investigative activities and with the participation of the court that issued the relevant ruling. A report shall be prepared on the destruction of the materials and shall be signed by the prosecutor and the judge. The report on the destruction of the materials, signed by the prosecutor and the judge, shall be submitted to the Personal Data Protection Inspector, to the Commission for Destroying Information / Personal Data Obtained as a Result of Operative- Investigative Activities and shall be entered into the Court Register of Secret Investigative Activities. 5. The unlawful restriction of the rights and freedoms of natural and legal persons by bodies (public servants) conducting operative-investigative activities shall carry liability under the legislation of Georgi a.	

Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**N/A**	**Article 137. Urgent storage of computer data** If there is reasonable cause to believe that computer data may be lost or changed, the person responsible for storing of the data may be instructed by the decree of the prosecutor to keep the data immediately for no more than 90 days. Natural or legal person storing such data is obliged to ensure the storage, integrity and protection of this computer data for the term provided by for in the decree. Subsequent request for production of stored computer data shall be conducted in accordance with Articles 112 and 136.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and	**N/A**	

other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.		
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the	**Criminal Procedure Code** **Article 136 - Requesting a document or information** 1. If there is 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, the prosecutor may file a motion with a court, according to the place of investigation, to issue a ruling requesting the provision of the relevant information or document. 2. If there exists reasonable cause to believe that a person is carrying out a criminal act through a computer system, the prosecutor may request a court, according to the place of investigation, to deliver a ruling ordering the service provider to provide information about the user. 3. For the purposes of this article, information about the user shall be any information that a service provider stores as computer data or in any other form that is related to the users of its services, differs fro m the internet traffic and content data and which can be used to establish/determin e:	**Article 3. Definition of basic terms for the purposes of this Code** 29. Service provider – person authorized by the Law on Electronic Communications of Georgia, as well as any natural or legal person which provides users with an opportunity to interact through a computer system, also any other person that processes or stores computer data on behalf of such communication services or of the consumers of such services (except state agency)." 30. Identification data of a user - the data envisaged by Paragraph z[72] of Article 2 of the Law of Georgia on Electronic Communications;" 34. Identification data of communication equipment – the data envisaged by Paragraph z[73] of the Law of Georgia on Electronic Communications; 40. Computer data storage device – any device that provides opportunity for recording and storage of computer data. **Article 136. Requesting a document**

technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	a) the type of communication services and technical means used, and the time of service; b) the identity of the user, mail or residential address, phone numbers and other contact details, information on accounts and taxes, which are available based on a service contract or agreement; c) any other information on the location of the installed communications equipment, which is available based on a service contract or agreement. 4. Provisions of Articles 143^2 - 143^{10} shall apply to the investigative actions stipulated by this article.	**or information** 1. If there is a reasonable cause to believe that electronic communications content data essential to the criminal case are stored in a computer system or on a computer data storage device of the service provider, the prosecutor may file a motion with a court, according to the place of investigation, to issue a ruling requesting the provision of the relevant data from the service provider. 2. If there is a reasonable cause to believe that data identifying electronic communication and essential to the criminal case is stored in a computer system of the service provider or in the central data bank of the relevant state agency authorized by Paragraph 35 of Article 3 of this Code, the prosecutor may file a motion with a court, according to the place of investigation, to issue a ruling requesting the provision of the relevant data from the service provider or authorized state agency provided by paragraph 35 of Article 3 of this Code. 3. If there exists reasonable cause to believe that a person is carrying out a criminal act through a computer system or information essential to the criminal case is stored in a computer system, the prosecutor or investigator is authorized to issue a decree requesting production of identification data of a user and/or identification data of communication equipment from the service provider or duly authorized state agency envisaged by Paragraph 35 of Article 3 of this Code. Execution of a prosecutor's and investigator's decree shall be mandatory.

		3. Investigative actions under the paragraph 2 of this Article may be executed if investigation has been initiated or criminal prosecution is conducted for an offence for which the Criminal Code of Georgia prescribes imprisonment. 4. In the event of requesting the information and/or document in the case provided for by Paragraph 1 or 2 of this Article the protocol on receiving of such request shall be drafted in accordance with requirements of Article 134 of this Code. 5. The actions provided for by Paragraph 2 of this Article shall be carried out only if they are stipulated under this Code and if they are necessary to achieve a legitimate goal in a democratic society, in particular, to ensure national or public security, to prevent public disorders or crime, to protect the country's economic interests and the rights and freedoms of other persons. 6. The action provided for by Paragraph 2 of this Article is necessary in a democratic society if they are carried out due to urgent public needs and if they constitute an adequate and proportional means for the achieving a legitimate goal. 7. The scope (intensity) of the action provided for by Paragraph 2 of this Article shall be proportionate to the legitimate goal. 8. The measures provided for by Paragraph 2 of this Article may be carried out only when the evidence cannot be obtained through other means or it requires unreasonably great effort.

		9. A person, who learns about conducting of a investigative actions in regard to him/her provided for by Paragraph 1 or 2 of this Article during the legal proceedings on a given case, may appeal the ruling authorizing an investigative action provided for by Paragraph 1 of this Article, in the investigative collegium of the relevant court of appeal within 48 hours after receipt of the above information and of being informed of the right to appeal the ruling. The annulment of the appealed ruling by the court of appeal and recognition of a conducted investigative action as unlawful shall serve as grounds for recognizing the information obtained as a result of that action as inadmissible evidence in the manner provided for by this Code. A decision reached by a court of appeal on the appeal may be used as a basis for a person to demand, under Article 7(3) of this Code, compensation for damages incurred as a result of the illegal obtaining, keeping or disclosure of information on the person's private life/ personal data. 10. A person who learns about the conduct of a investigative action against him/her provided for by Paragraph 1 or 2 of this Article after the completion of legal proceedings in a given case, may appeal the ruling authorizing investigative action provided for by Paragraph 1 of this Article in the investigative board of the relevant court of appeal within one month after receiving of the above information and of being informed of the right to appeal the ruling. The recognition as unlawful by a court of appeal of a conducted secret

		investigative action may be considered as newly discovered circumstances provided for by Article 310(h) of this Code, which may serve as grounds for the revision of a judgement, provided the evidence obtained as a result of that secret investigative action served as grounds for that judgement. A decision made by a court of appeal on the appeal may be used as a basis for a person to demand, under Article 7(3) of this Code, compensation for damages as a result of her illegal obtaining, keeping or disclosure of information on the person's private life/ personal data. 11. In the appeal referred to in Paragraphs 9 and 10 of this Article, reference shall be made to the breach of the procedure established under this ***Article*** for the conduct of an investigative action. An appeal shall be filed with the court that rendered the ruling. The investigative boards of a court of appeal shall review an appeal not later than 72 hours after it has been filed. A court of appeal shall, by notification, ensure the participation of the appellant and the prosecution in the review of the appeal. Their non-appearance shall not preclude the review of the appeal. A decision made on the appeal shall be publicly announced and, if so requested, it shall be handed over to the appellant and the prosecution. 12. An investigative action provided for by Paragraph 1 of this Article, against a state political official, a judge and a person having immunity may be carried out under a ruling of a judge of the Supreme Court of Georgia, or upon a reasoned motion of

		the Chief or Deputy Chief Prosecutor of Georgia. 14. The court shall review a motion stipulated by Paragraph 2 of this Article in the manner prescribed by Article 112 of this Code. 15. Provisions of par. 2-5 of Article 143^{2}, par. 5, 5^{1}, 5^{2} and 14-17 of Article 143^{3}, Articles 143^{8} and 143^{9} shall apply to the investigative actions stipulated by paragraph 1 of this article. 16. Article 6, par. (d)(a) of the Law on State Secret of Georgia does not apply to investigative actions provided by par. 1 of the Article 136 of this Code. **Law of Georgia on Electronic Communications** **Article 2. Definition of terms used in the Law** "z^{72}) Identification data of a user –any information that a service provider stores as computer data, or in any other form that is related to the users of its services, differs from the internet traffic data and which can be used to establish/determine: the type of communication services; the identity of the user, mail or residential address, phone number and other contact details, information on accounts and taxes, which are available based on a service contract or agreement; any other information on the location of the installed communications equipment, which is available based on a service contract or agreement. z^{73}) Identification data of communication

		equipment – any data that enables individual identification of communication equipment (including the phone number, address of Internet protocol, International Mobile Station Equipment Identity (EMEI), international mobile subscriber identity (IMSI), MAC address, etc.)
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer	***Criminal Procedure Code*** **Article 119. The Purpose and Grounds for Search and Seizure** 1. If there is a probable cause, a search shall be conducted for the purpose of uncovering and seizing an item, document, substance or any other object containing information that is essential to the case. 2. A search may also be conducted to find a wanted perso n or a corpse. 3. An item, document, substance or any other object containing information that is essential to the case may be seized if there is probable cause that it is kept in a certain place, with a certain person and if there i s no need to search for it 4. A search to seize an item, document, substance or any other object containing information that is important for the case may be conducted, if there is probable cause that it is kept in a certain place, with a cer tain person and if search is necessary to discover it. **Article 120. The Rule for Search and Seizure** 1. Based on a court ruling authorising search or seizure or, in the case of urgent necessity, based on a decree of an investigator, an investigator may enter a storage facility, a dwelling place, a storage room or other property to locate and seize an item, document, substance or any other object containing information. 2. Before starting a seizure or search, an investigator shall	

data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	be obliged to present a court order, or in the case of urgent necessity, a decree, to a person subjected to the seizure or search. The presentation of the ruling (decree) shall be confirmed by the signature of the person subject to search. 3. An investigator may forbid the persons who are present or who arrive at the place of search, to leave the place, to interact with each other or with any other person before the search is completed, which sh all be recorded in the appropriate record. 4. After a ruling, or in the case of urgent necessity, a decree, is presented, an investigator shall offer the person subject to the search, to voluntarily turn over an item, document, substance or any other object containing information that is subject to seizure. If an object that is subject to seizure is voluntarily provided, that fact shall be recorded in the relevant record. In the case of refusal to voluntarily turn over the requested object, or in the case of its incomplete provision, it shall be seized by coercion. 5. During a search, an item, document, substance or any other object containing information that is referred to in a ruling or decree shall be searched for and seized. Also, all other objects containing information that may be of an evidentiary value for that case, or that clearly indicates another offence, as well as an item, document, substance or any other object containing information that has been withdrawn from civil circulation. 6. An item, document, substance or any other object containing information that has been detected during a search or seizure, shall, if possible, be presented, before its seizure, to persons participating in that investigative action. Then, it shall be seized, described in detail, sealed and if possible, packaged. On the packaged item, in addition to a seal, the date and signatures of the persons	

	who participated in the investigative action shall be indicated. A document that is seized due to its contents, s hall not be sealed. 7. During a search or seizure, an investigator may open a closed storage facility, dwelling place and premises, if the person subject to search refuses to voluntarily open them. 8. A person present at the place of search and/or seizure may be personally searched if there is a probable cause that he/she has concealed an item, document, subject or any other object that is subject to seizure. Such case shall be considered an urgent necessity and a personal search shall be conducted without a court ruling. The lawfulness of the se arch and/or seizure shall be examined by the court in the manner provided for by this Code. 9. A search or seizure of a legal person or in a building of an administrative body shall be conducted in the presence of its head or representative. 10. A prosecutor shall have the right to primary examination of an object, item, substance, or document containing information seized upon motion of the defence.	
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the	**Criminal Procedure Code** **Article 137 - Real time collection of internet traffic data** 1. If there is reasonable cause to believe that a person is carrying out a criminal act through a computer system, the prosecutor may, according to the place of investigation, file a motion with a court for a ruling authorising a real-time collection of internet traffic data; under the ruling the service provider is obliged to collaborate with the investigation authorities and assist them, in real time, in the collection or recording of those internet traffic data that are related to specific communications performe d in the territory of Georgia and transmitted through a co	

collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	mputer system. 2. A motion specified in paragraph 1 of this article shall take account of the technical capacities of the service provider to collect and record internet traffic data in real time. The period for collecting and recording internet traffic data in real time shall not be longer than the period required to obtain evidence for a criminal case. 3. Provisions of Articles 143^{2}-143^{10} shall apply to the investigative actions stipulated by this article. **Law on Operative-Investigative Activity** **Article 7 - Concept of an operative-investigative measure** 1. An operative-investigative measure is an action carried out by a state body or an official duly authorised under this Law, who/which, within the scope of his/her/its powers, ensures the fulfilment of the objecti ves specified in Article 3 of this Law. 2. In order to accomplish these objectives, the bodies con ducting operative- investigative activities may, overtly or covertly: a) interview a person; b) collect information and conduct surveillance; c) carry out a test purchase; d) carry out a controlled delivery; e) examine objects and documents; f) identify a person; g) censor the correspondence of an arrested, detained and convicted person; h) obtain electronic communication identification data; i)(Deleted - 1.8.2014, No 2635). j) infiltrate a secret collaborator or an operative into a cri minal group in a prescribed manner; k) set up an undercover organisation in a prescribed mann er;	

	l) monitor Internet communications by observing and participating in open **and closed** Internet communications in the global information network (Internet), and creating situations of the illegal obtaining of computer data in order to identify a perpetrator. ***[(the normative content related to the words of the same provision 'observe internet communications' shall be repealed) - decision No1/2/519 of the Constitutional Court of Georgia of 24 October 2012 – website 30.10.2012წ.]*** 3. A body conducting operative-investigative activities may, in accordance with the procedure laid down in Chapter XVI[1] of the Criminal Procedure Code of Georgia, obtain electronic communication identification data from an electronic communications company in the following cases: when searching for a missing person; when searching for an accused or convicted person for the purpose of bringing him/her before a relevant state authority if such person avoids the application of coercive measures imposed on him/her or the serving of an imposed sentence; when searching for property lost as a result of a crime. 3[1]. The operative-investigative measures specified in paragraph 2(h) and (i) of this article may also be conducted in respect of a judge by an order of the chairperson of the Supreme Court upon a reasoned reques t of the Chief Prosecutor of Georgia. 4. (Deleted - 1.8.2014, No 2635). 5. (Deleted - 1.8.2014, No 2635). 6. The list of measures specified in paragraph 2 of this arti cle may be changed or supplemented only under this Law. 7. A report shall be prepared at the time of conducting an operative-investigative measure; the report shall describe the circumstances in which technical means were used. The report, along with the obt ained materials, shall be stored in accordance with this La	

	w. 8. An official of the body conducting an operative-investigative activity shall personally participate in the conduct of the measures specified in paragraph 2 of this article, and at the same time, such official may use the assistance of specialists in a specific field, and the voluntary overt or covert assistance of certain persons.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.	**Criminal Procedure Code** **Article 138 - Obtaining content data** 1. If there exists reasonable cause to believe that a person is carrying out a criminal act through a computer system, the prosecutor may, according to the place of investigation, file a motion with a court for a ruling authorising the collection of content data in real time; under the ruling the service provider is obliged to collaborate with the investigation authorities and assist them, in real time, in the collection or recording of content data related to specific communications performed in the territory of Georgia and transmitted through a computer system. 2. A motion specified in paragraph 1 of this article shall take account of the technical capacities of a service provider to collect and record content data in real time. The period for real-time collection and recording of content data shall not be longer than the period required to obtain evidence for a criminal case. 3. Provisions of Articles 143^{2}-143^{10} shall apply to the investigative actions stipulated by this article. **Article 143^{1}.Types of secret investigative actions** 1. Types of secret investigative actions shall include: a) secret eavesdropping and recording of phone conversations; b) removal and recording of information from a communications channel (by connecting to the	

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	communication facilities, computer networks, line communications and station devices), computer system (both directly and remotely) and installation of respective software in the computer system for this purpose; c) monitoring of post and telegraphic communications (except for a diplomatic post); d) secret video and audio recording, film and photo shooting; e) electronic surveillance through technical means, which do not endanger human life, health or the environment. 2. It shall be permissible to carry out several investigative actions at the same time. **Law on Operative-Investigative Activity** **Article 7 - Concept of an operative-investigative measure** 1. An operative-investigative measure is an action carried out by a state body or an official duly authorised under this Law, who/which, within the scope of his/her/its powers, ensures the fulfilment of the objecti ves specified in Article 3 of this Law. 2. In order to accomplish these objectives, the bodies con ducting operative- investigative activities may, overtly or covertly: a) interview a person; b) collect information and conduct surveillance; c) carry out a test purchase; d) carry out a controlled delivery; e) examine objects and documents; f) identify a person; g) censor the correspondence of an arrested, detained and convicted person; h) obtain electronic communication identification data; i)(Deleted - 1.8.2014, No 2635). j) infiltrate a secret collaborator or an operative into a cri	

	minal group in a prescribed manner; k) set up an undercover organisation in a prescribed mann er; l) monitor Internet communications by observing and participating in open and closed Internet communications in the global information network (Internet), and creating situations of the illegal obtaining of computer data in order to identify a perpetrator. ***[(the normative content related to the words of the same provision 'observe internet communications' shall be repealed) - decision No1/2/519 of the Constitutional Court of Georgia of 24 October 2012 – website 30.10.2012ფ.]*** 3. A body conducting operative-investigative activities may, in accordance with the procedure laid down in Chapter XVI[1] of the Criminal Procedure Code of Georgia, obtain electronic communication identification data from an electronic communications company in the following cases: when searching for a missing person; when searching for an accused or convicted person for the purpose of bringing him/her before a relevant state authority if such person avoids the application of coercive measures imposed on him/her or the serving of an imposed sentence; when searching for property lost as a result of a crime. 3[1]. The operative-investigative measures specified in paragraph 2(h) and (i) of this article may also be conducted in respect of a judge by an order of the chairperson of the Supreme Court upon a reasoned reques t of the Chief Prosecutor of Georgia. 4. (Deleted - 1.8.2014, No 2635). 5. (Deleted - 1.8.2014, No 2635). 6. The list of measures specified in paragraph 2 of this arti cle may be changed or supplemented only under this Law. 7. A report shall be prepared at the time of conducting an operative-investigative measure; the report shall describe	

	the circumstances in which technical means were used. The report, along with the obtained materials, shall be stored in accordance with this Law. 8. An official of the body conducting an operative-investigative activity shall personally participate in the conduct of the measures specified in paragraph 2 of this article, and at the same time, such official may use the assistance of specialists in a specific field, and the voluntary overt or covert assistance of certain persons.	

ANNEXES

Draft

LAW OF GEORGIA
ON AMENDMENTS TO THE LAW OF GEORGIA
ON ELECTRONIC COMMUNICATIONS

Article 1. The law of Georgia on Electronic Communications shall be amended as follows:

1. Subparagraphs z^{72-76} shall be added to the Article 2 with the following wording:

"z^{72}) Identification data of a user –any information that a service provider stores as computer data, or in any other form that is related to the users of its services, differs from the internet traffic data and which can be used to establish/determine: the type of communication services; the identity of the user, mail or residential address, phone number and other contact details, information on accounts and taxes, which are available based on a service contract or agreement; any other information on the location of the installed communications equipment, which is available based on a service contract or agreement.

z^{73} - Identification data of communication equipment – any data that enables individual identification of communication equipment (including the phone number, address of Internet protocol, International Mobile Station Equipment Identity (EMEI), international mobile subscriber identity (IMSI), MAC address, etc.)

LAW OF GEORGIA
ON AMENDMENTS TO CRIMINAL PROCEDURE CODE OF GEORGIA

Article 1. The Criminal Procedure Code shall be amended as follows:

a. Paragraph 29 of Article 3 shall be set forth as follows:

"29. Service provider – person authorized by the Law on Electronic Communications of Georgia, as well as any natural or legal person which provides users with an opportunity to interact through a computer system, also any other person that processes or stores computer data on behalf of such communication services or of the consumers of such services (except state agency)."

b. Paragraph 30 of Article 3 shall be set forth as follows:
"30. Identification data of a user - the data envisaged by Paragraph z^{72} of Article 2 of the Law of Georgia on Electronic Communications;"

c. Paragraph 34(**?**) shall be added to Article 3 with the following wording:
"34. Identification data of communication equipment – the data envisaged by Paragraph z^{73} of the Law of Georgia on Electronic Communications;"

d) Paragraph 40(**?**) shall be added to Article 3 with the following wording:
"40. Computer data storage device – any device that provides opportunity for recording and storage of computer data."

2. Articles 136 and 137 shall be set forth as follows:

"Article 136. Requesting a document or information

1. If there is a reasonable cause to believe that electronic communications content data essential to the criminal case are stored in a computer system or on a computer data storage device of the service provider, the prosecutor may file a motion with a court, according to the place of investigation, to issue a ruling requesting the provision of the relevant data from the service provider.

2. If there is a reasonable cause to believe that data identifying electronic communication and essential to the criminal case is stored in a computer system of the service provider or in the central data bank of the relevant state agency authorized by Paragraph 35 of Article 3 of this Code, the prosecutor may file a motion with a court, according to the place of investigation, to issue a ruling requesting the provision of the relevant data from the service provider or authorized state agency provided by paragraph 35 of Article 3 of this Code.

3. If there exists reasonable cause to believe that a person is carrying out a criminal act through a computer system or information essential to the criminal case is stored in a computer system, the prosecutor or investigator is authorized to issue a decree requesting production of identification data of a user and/or identification data of communication equipment from the service provider or duly authorized state agency envisaged by Paragraph 35 of Article 3 of this Code. Execution of a prosecutor's and investigator's decree shall be mandatory.

3. Investigative actions under the paragraph 2 of this Article may be executed if investigation has been initiated or criminal prosecution is conducted for an offence for which the Criminal Code of Georgia prescribes imprisonment.

4. In the event of requesting the information and/or document in the case provided for by Paragraph 1 or 2 of this Article the protocol on receiving of such request shall be drafted in accordance with requirements of Article 134 of this Code.

5. The actions provided for by Paragraph 2 of this Article shall be carried out only if they are stipulated under this Code and if they are necessary to achieve a legitimate goal in a democratic society, in particular, to ensure national or public security, to prevent public disorders or crime, to protect the country's economic interests and the rights and freedoms of other persons.

6. The action provided for by Paragraph 2 of this Article is necessary in a democratic society if they are carried out due to urgent public needs and if they constitute an adequate and proportional means for the achieving a legitimate goal.

7. The scope (intensity) of the action provided for by Paragraph 2 of this Article shall be proportionate to the legitimate goal.

8. The measures provided for by Paragraph 2 of this Article may be carried out only when the evidence cannot be obtained through other means or it requires unreasonably great effort.

9. A person, who learns about conducting of a investigative actions in regard to him/her provided for by Paragraph 1 or 2 of this Article during the legal proceedings on a given case, may appeal the ruling authorizing an investigative action provided for by Paragraph 1 of this Article, in the investigative collegium of the relevant court of appeal within 48 hours after receipt of the above information and of being informed of the right to appeal the ruling. The annulment of the appealed ruling by the court of appeal and recognition of a conducted investigative action as unlawful shall serve as grounds for recognizing the information obtained as a result of that action as inadmissible evidence in the manner provided for by this Code. A decision reached by a court of appeal on the appeal may be used as a basis for a person to demand, under Article 7(3) of this Code, compensation for damages incurred as a result of the illegal obtaining, keeping or disclosure of information on the person's private life/ personal data.

10. A person who learns about the conduct of a investigative action against him/her provided for by Paragraph 1 or 2 of this Article after the completion of legal proceedings in a given case, may appeal the ruling authorizing investigative action provided for by Paragraph 1 of this Article in the investigative board of the relevant court of appeal within one month after receiving of the above information and of being informed of the right to appeal the ruling. The recognition as unlawful by a court of appeal of a conducted secret investigative action may be considered as newly discovered circumstances provided for by Article 310(h) of this Code, which may serve as grounds for the revision of a judgement, provided the evidence obtained as a result of that secret investigative action served as grounds for that judgement. A decision made by a court of appeal on the appeal may be used as a basis for a person to demand, under Article 7(3) of this Code, compensation for damages as a result of her illegal obtaining, keeping or disclosure of information on the person's private life/ personal data.

11. In the appeal referred to in Paragraphs 9 and 10 of this Article, reference shall be made to the breach of the procedure established under this ***Article*** for the conduct of an investigative action. An appeal shall be filed with the court that rendered the ruling. The investigative boards of a court of appeal shall review an appeal not later than 72 hours after it has been filed. A court of appeal shall, by notification, ensure the participation of the appellant and the prosecution in the review of the appeal. Their non-appearance shall not preclude the review of the appeal. A decision made on the appeal shall be publicly announced and, if so requested, it shall be handed over to the appellant and the prosecution.

12. An investigative action provided for by Paragraph 1 of this Article, against a state political official, a judge and a person having immunity may be carried out under a ruling of a judge of the Supreme Court of Georgia, or upon a reasoned motion of the Chief or Deputy Chief Prosecutor of Georgia.

13. If the information or documents essential to the criminal case are not stored in a computer system or on a computer data carrier or in the central bank of data of the relevant state agency authorized envisaged by Paragraph 35 of Article 3 of this code, is obtained in the manner prescribed by Articles 119, 120, 125 and 126 of this Code. (**This provision seems to be deleted from the revised draft**)

14. The court shall review a motion stipulated by Paragraph 2 of this Article in the manner prescribed by Article 112 of this Code.

15. Provisions of par. 2-5 of Article 143^2, par. 5, 5^1, 5^2 and 14-17 of Article 143^3, Articles 143^8 and 143^9 shall apply to the investigative actions stipulated by paragraph 1 of this article.

16. Article 6, par. (d)(a) of the Law on State Secret of Georgia does not apply to investigative actions provided by par. 1 of the Article 136 of this Code.

Article 137. Urgent storage of computer data

If there is reasonable cause to believe that computer data may be lost or changed, the person responsible for storing of the data may be instructed by the decree of the prosecutor to keep the data immediately for no more than 90 days. Natural or legal person storing such data is obliged to ensure the storage, integrity and protection of this computer data for the term provided by for in the decree. Subsequent request for production of stored computer data shall be conducted in accordance with Articles 112 and 136.

Previous assessments

3271_cybercrime EAP Report Part II_ 2

Current legislation

Criminal Procedure Code.pdf

Electronic Communications Law.

Law on Operative Activity.pdf