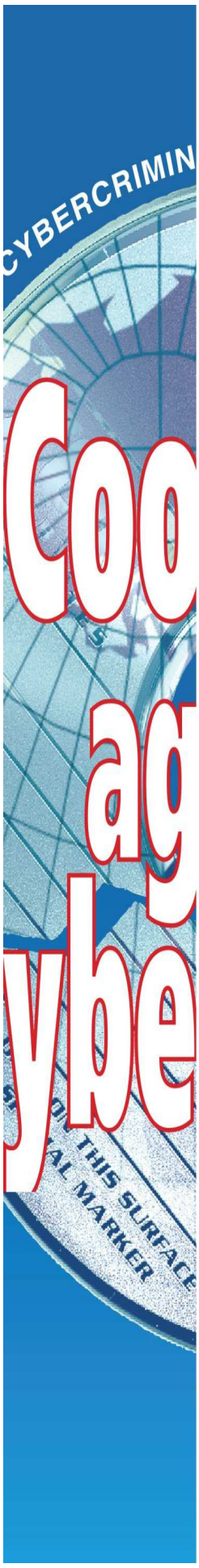


**CyberCrime@EAP**

**EU/COE Eastern Partnership – Council of Europe Facility: Cooperation against Cybercrime**

# Article 15 – Safeguards in the Eastern Partnership region

Discussion paper

prepared under the CyberCrime@EAP project by:

Prof.dr.sc. Dražen Dragičević, Professor at University of Zagreb, Faculty of Law, Croatia
and
Marko Jurić, Research and teaching assistant at University of Zagreb, Faculty of Law, Croatia

Data Protection and Cybercrime Division
Council of Europe
Strasbourg, France, Version 1 October 2013 (provisional)

**www.coe.int/cybercrime**

Funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

**For further information please contact:**

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
Strasbourg, France

Tel: +33-3-8841-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

**Disclaimer:**

This technical report does not necessarily reflect official positions of the Council of Europe or of the European Union or of the Parties to the agreements referred to.

**TABLE OF CONTENTS**

**LIST OF ABBREVATIONS**

| | |
|---|---|
| Article 15, 16, 17, 18, 19, 20, 21 | Respective articles of the Convention on Cybercrime |
| article X/Y | article X, paragraph Y of the applicable legal instrument |
| Convention | Convention on Cybercrime |
| ECHR | Convention for the Protection of Human Rights and Fundamental Freedoms |
| ECtHR | European Court of Human Rights |
| Section 2 | Section 2 of the Convention on Cybercrime |
| ArCPC | Armenian Code on Criminal Procedure |
| ArCC | Armenian Criminal Code |
| ArLOSA | Armenian Law on Operative-Search Activity |
| AzCPC | Azeri Code on Criminal Procedure |
| AzDSAA | Azeri Detective-Search Activity Act |
| AzICIA | Azeri Law on Intelligence and Counter-Intelligence Activities |
| ByCPC | Belarus Code of Criminal Procedure |
| GeCPC | Georgian Criminal Procedure Code |
| GeLOSA | Georgian Law on Operative Search Activity |
| MdLPCC | Moldovan Law on Preventing and Combating Cybercrime |
| MdCPC | Moldovan Criminal Procedure Code |
| MdLSIA | Moldovan Law on Special Investigative Activity |
| UaCPC | Ukrainian Criminal Procedure Code |

# Executive summary

According to Article 15 of the Budapest Convention on Cybercrime, the procedural powers adopted by Parties to the Convention are to be "subject to conditions and safeguards provided for under its domestic law which shall provide for the adequate protection of human rights and liberties...".

The purpose of the present report is to help ensure that appropriate conditions and safeguards are established when Parties to the Budapest Convention implement the procedural powers foreseen under Articles 16 to 21 of this treaty.

The present study covers the States participating in the CyberCrime@EAP project, that is, Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine.[1]

**Expedited preservation of stored computer data (Article 16)**

None of the project countries implemented Article 16 as a standalone measure. As regards Armenia, Belarus and Ukraine, significant changes are needed in order to bring their legislation in line with Article 16. The Republic of Moldova is partially in line with the Convention, but should broaden the scope of its legislation in order to give full effect to Article 16. Azerbaijan and Georgia use production orders to achieve the purpose of Article 16 in a manner consistent with the requirements of the Convention.

For all of the project countries, we recommend the implementation of Article 16 as a standalone measure. This would help not only help secure electronic evidence but also strengthen rule of law and human rights safeguards.

**Expedited preservation and partial disclosure of traffic data (Article 17)**

Azerbaijan, Georgia and the Republic of Moldova are in line with Article 17. On the other side, Armenia, Belarus and Ukraine should make significant changes in order to bring their legislation in line with Article 17. For all of the project countries, except the Republic of Moldova, we recommend that specific partial disclosure orders be implemented. This would help strengthen rule of law and human rights safeguards.

**Production order (Article 18)**

With the exception of Georgia, all of the project countries should make significant changes in their legislation in order to bring it completely in line with Article 18. In general, project countries (with the exception of Georgia and, partially, Azerbaijan) use a combination of rules on seizure and specific provisions regulating the production of information which could qualify as subscriber information.

For all of the project countries, except Georgia, we recommend that extensive analyses of their legislation be undertaken in the light of Article 18 and that specific rules on the production of computer data be implemented. For Georgia, we recommend that the scope of provisions which implements Article 18/2 be broadened, in accordance with Article 14.

**Search and seizure of stored computer data (Article 19)**

Project countries did not implement specific provisions on computer-related search and seizure. In all of the surveyed countries, "traditional" rules on search and seizure are used to inspect

[1] The present discussion paper complements an earlier study covering the Netherlands, the USA and Croatia. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

computer systems and data contained in them. In general, project countries have adequate conditions and safeguards in place with regard to grounds justifying application of the measures and exemptions in favor of certain persons or places from the application of the measure. With regard to Belarus, the issue of the absence of judicial overview should be resolved; obviously this question is larger than the question of Article 15.

In particular, however, project countries should give effect to the requirements arising under paragraphs 2-4 of the Article 19 and develop specific conditions and safeguards in relation to these powers.

**Real-time collection of traffic data (Article 20) and interception of content data (Article 21)**

Project countries, with the exception of Georgia, do not make significant differences between the collection of traffic data in real time and the interception of content data. As regards the collection of traffic data, it should be noted that in some of the project countries specific systems of data retention are in place (Azerbaijan, Belarus, Ukraine) so there is no practical need for the strict application of the Article 20. On the other hand, in Armenia the collection of traffic data in real time is possible only in accordance with the same rules that govern the interception of content data.

As regards the interception of content data, project countries in general have adequate systems of conditions and safeguards in place. In that context, the requirements of open criminal investigation, judicial supervision or limitations of the duration of the measure are in place. In all of the countries, except Georgia, the interception of a communication is reserved for a limited catalogue of serious criminal offences. The situation in Belarus, regarding absence of judicial supervision, should be addressed in the course of more broad discussions regarding the criminal justice system in that country.

In relation to all of the project countries, additional efforts could be made in order to bring their legislation on interception of communications more in line with the requirements of precision and foreseeability, established by the case law of the European Court of Human Rights.

# 1 Introduction

## 1.1 CyberCrime@EAP project

The Project on Cooperation against Cybercrime is one of four projects under the Eastern Partnership Facility of the European Union and the Council of Europe. The project started on 1 March 2011, has a duration of thirty months (1 March 2011 – 31 August 2013) and a budget of 724,040 Euro. It is implemented by the Council of Europe in the Eastern Partnership countries Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine.

The specific project purpose is to strengthen the capacities of criminal justice authorities of the Eastern Partnership countries to cooperate effectively against cybercrime in line with European and international instruments and practices.

Under Result 2 – Eastern Partnership countries are provided with the tools for action against cybercrime – the project supports measures to strengthen the national legislations on cybercrime through defining country-specific needs as well as to assist the understanding and discussion of the challenges of the application of the Convention on Cybercrime (CETS 185).

States have a positive obligation to protect the rights of individuals. This includes their protection against crime but also against arbitrary interference by public authorities.

The Budapest Convention on Cybercrime helps states meet this challenge with regard to cybercrime: it requires governments to take measures against offences against and by means of computer data and systems, to provide law enforcement with procedural powers for effective investigations and to engage in efficient international cooperation.

At the same time, Article 15 protects individuals against arbitrary intrusion: the procedural powers adopted by Parties to the Convention are to be "subject to conditions and safeguards provided for under its domestic law which shall provide for the adequate protection of human rights and liberties".

The Council of Europe addresses this question when supporting countries in the implementation of the Budapest Convention through its capacity building programmes on cybercrime. Within the framework of the joint project, CyberCrime@IPA on cooperation against cybercrime in South-eastern Europe (including Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo[2]) a discussion paper was drafted on Safeguards and Conditions – Article 15 of the Budapest Convention[3]. The purpose of this report therefore is to further advance the discussion on this complex issue by sharing experience in the project region and beyond. It may help "operationalise" the general principles of Article 15 in view of assessing and supporting their implementation in different countries.

In order to assess the current level of implementation of the provisions under Article 15 in the Eastern Partnership Region, the Secretariat prepared and circulated a questionnaire among the project countries of the CyberCrime@EAP project.

[2] All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.

[3] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

An International Conference on Safeguards and Conditions[4] was organised by the CyberCrime@IPA and CyberCrime@EAP projects in Baku, Azerbaijan, 5 November 2012. The conference reviewed how conditions and safeguards are implemented in countries of Eastern and South-eastern Europe.

A follow up Roundtable Discussion was held in Strasbourg, France on 7 December 2012, in order to complete and discuss in detail the status of implementation of Article 15 of the Budapest Convention in the Eastern Partnership Region.

## 1.2 The aim of this report

The objective of this report is twofold:

- To analyze the legal framework of the Eastern Partnership (EAP) countries with regard to the requirements set by Article 15 of the Convention on Cybercrime; and
- To provide recommendations for EAP countries regarding the strengthening their national legislation on cybercrime with special regard to the application of safeguards and conditions required by Article 15.

## 1.3 Available information

In order to gather information necessary for this report, a questionnaire was sent to the project countries with inquiries regarding implementation of Section 2 of the Convention in their domestic legislations. Replies were received from Armenia, Azerbaijan, Georgia and the Republic of Moldova. With the aim of discussing some of the issues which were not addressed in the replies to the questionnaire, as well as to gather information regarding the legislation of the countries that did not reply to the questionnaire, a roundtable discussion on Article 15 of the Budapest Convention was organized in Strasbourg, France, on 7 December 2012. Representatives from the project countries, except for Belarus, participated in this meeting. In addition, translations of certain national sources of law, or their excerpts, as well as some other documents, were provided by the CoE Secretariat. All of these sources are indicated at the beginning of every country profile.

All of the information was provided in English. For some of the sources unofficial translations of the national legal instruments were made available. In other cases, authors have relied on the assistance of representatives of project countries to obtain translation of particular provisions of their national legislation. Being very well aware of the complexity and difficulty of the translation of legal texts, the authors would like to express their gratitude to the representatives of the project countries, who have invested time and efforts in order to provide explanations of their national law.

## 1.4 Structure of this report

In the next section of this report we have provided some explanations regarding the subject-matter, purpose and scope of Article 15 and specific measures defined in Section 2 of the Convention.

In the following sections (2-7), legal framework of every project country is being analysed.

Key findings, providing overview of implementation of Articles 16-21, are summarized in section 8.

[4] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_project_Phase3_2571/2571_IGF_WS_art15_outline_v8_31oct12%20(2).pdf

## 1.5 General information regarding Section 2 Budapest Convention and Article 15

The Budapest Convention on Cybercrime, in its Section 2 (Procedural law), provides for a series of procedural powers which are considered necessary to effectively combat cybercrime and other criminal offences involving electronic evidence by facilitating their detection, investigation and prosecution at the domestic and international level.

These procedural powers are defined in articles 16-21 of the Convention. Their application, however, is limited by the Convention's provisions on the scope of application of its procedural law (article 14) and by the requirement that establishment, implementation and application of powers defined in articles 16-21 be balanced with the requirement of adequate protection of human rights and liberties (article 15). As was explained supra, the purpose of this report is to analyse the implementation of Section 2 in the countries of the EAP project, with special emphasis on the fulfilment of requirements arising from Article 15.

Article 15 reads as follows:

> 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, responsibilities and legitimate interests of third parties.

In order to give effect to Article 15, Parties to the Convention should therefore limit the establishment, implementation and application of measures defined in Articles 16-21 by a series of conditions and safeguards. These conditions and safeguards can be established in the domestic law of every Party by constitutional, legislative, judicial or other means.[5]

While the Convention is very clear in its requirement that procedural measures be balanced with the requirements of human rights protection, it is arguably much more abstract when it comes to defining the conditions and safeguards which should be used to that effect. The reason for such an approach was the fact that Convention is designed to be applicable in different legal systems and cultures; therefore, it was not possible to specify in detail what are the conditions and safeguards applicable for each power or procedure.

For the aforementioned reasons, it is the responsibility of the Parties to ensure that they follow conditions and safeguards which might be applicable in their legal system. However, Parties were not left without any guidance in this task.

[5] Explanatory report - paragraph 145.

In general, article 15 mandates that the Parties should adhere to the (1) obligations arising under applicable international human rights instruments. For member states of the Council of Europe, this is obviously Convention for the Protection of Human Rights and Fundamental Freedoms, but also some other legal instruments.[6] In addition, article 15/1 stipulates that whatever the obligations of international treaties are applicable they should in any case incorporate the (2) principle of proportionality.

In addition to these general requirements, Convention (in the article 15/2) provides that conditions and safeguards shall, "as appropriate in view of the nature of the procedure or power concerned, inter alia, include" (3) judicial or other independent supervision, (4) grounds justifying application, and (5) limitation of the scope and the duration of such power or procedure.

Furthermore, the structure and the subject-matter of the procedural measures in the Convention can be considered as a specific safeguard per se. Since the Convention provides for six measures, with various levels of intrusiveness, it can very well be argued that the implementation of all of the measures in Section 2 enables the authorities to use the measure which is least intrusive, and thereby contributes to the protection of human rights and liberties.[7]

### 1.5.1 Convention for the Protection of Human Rights and Fundamental Freedoms

As mentioned above, the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) is the most important source of law for protection of human rights and liberties in Europe. In the context for this report, this convention protects several fundamental rights and liberties: Rights to liberty and security (article 5) and fair trial (article 6), principle of no punishment without law (article 7) and the right to respect for private and family life (article 8).[8]

### 1.5.2 Principle of proportionality

According to the Explanatory report, the principle of proportionality should be implemented "by each Party in accordance with relevant principles of its domestic law".[9] For European countries, this principle derives from the "principles of… ECHR, its applicable jurisprudence and national legislation and jurisprudence". [10] Principle of proportionality requires that "the power or procedure … be proportional to the nature and circumstances of the offence". [11]

One specific instance of use of proportionality principle can be found with regard to Article 21, where the Convention on Cybercrime itself provides limitations in relation to the measure of interception of communications and stipulates that such measure should be used only for investigation and prosecution of limited number of criminal offences.

### 1.5.3 Case-law of the European Court of Human Rights

The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Convention on Cybercrime and other sources of Council of Europe's law are living legal instruments; they find their application, among other means, through the case-law of the European Court of Human Rights (ECtHR).

---

[6] In the legal system of the CoE, attention should be given also to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[7] See in ITU Study: „An important aspect related to the system of safeguards provided by the Council of Europe Convention on Cybercrime is the fact that the ability of law-enforcement agencies to use the instruments in a flexible way on the one hand and the guarantee of effective safeguards on the other depends on the implementation of a graded system of safeguards."

[8] Cf. Article 15 discussion paper, p. 10.

[9] Explanatory report, para. 146.

[10] Explanatory report, para. 146.

[11] Explanatory report, para. 146.

Unfortunately, provisions of Convention on Cybercrime have until now not been analyzed in detail in the case-law of the ECtHR. To our best knowledge, the only case that refers directly to this Convention was K.U. v. Finland, from 2008.[12] This case concerned a minor (12 years old) whose age, detailed description of his physical characteristics, a link to the web page he had at the time, which showed his picture, as well as his telephone number (which was accurate save for one digit) have been published on the Internet dating site by an unknown person, which constituted a criminal offence of misrepresentation. In order to investigate the matter and identify the suspect, police had to gain access to the identity of the owner of the dynamic IP-address, held by the ISP. However, ISP declined to submit necessary data, regarding itself bound by the confidentiality of telecommunications as defined by law.[13] In the subsequent court proceedings, district and the supreme court have confirmed the position of the ISP, on the basis that "there was no explicit legal provision authorizing [the court]… to order the service provider to disclose telecommunications identification data". In the context of the Convention on cybercrime, this judgment is relevant for the interpretation of provisions on production of stored computer data (article 18). According to the legal reasoning of the ECtHR, the object of ECHR's article 8 is not only a negative obligation to the State to abstain from interference but also "positive obligations inherent in an effective respect for private or family life".[14] For these reasons, the ECtHR concluded that "practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator". In addition, the court argued that "although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others…", therefore, "… it is the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context.".

In addition, the ECtHR has developed significant case-law in the relation to various measures of surveillance of communications. Some of the decisions relevant in this context will be mentioned below.

### 1.5.4 Expedited preservation of stored computer data (Article 16)

Article 16 of the Convention regulates expedited preservation of stored computer data[15]; in conjunction with article 17 it also enables preservation of communication's traffic data[16]. Procedural powers defined in these two articles are specifically designed for the application in the digital environment and have no "traditional" counterpart in some other criminal procedure measure. While it is recognized that they can serve a very useful role in the catalogue of measures of criminal prosecution, the fact is that these measures have so far been implemented only by limited number of the Parties to the Convention.[17] Even more, there are still some open questions

[12] Application no. 2872/02.

[13] Para 6-9 of the judgment.

[14] Para. 42. of the judgment.

[15] According to Convention's article 1(b), „"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function".

[16] According to Convention's article 1(d), „"traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service".

[17] See in Schulman, Global State of Cybercrime Legislation, 2012., presentation available at http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus2012/presentations/WS1_coe_cyber_Octopus_ws%201_6June12.pdf; p. 9., also T-CY Assessment report regarding „Implementation of the preservation provisions of the Budapest Convention on Cybercrime", para. 11.

as to what amounts to correct implementation of article 16. In addition to this issue, during the discussions held for the preparation of this Report it became obvious that there exists a misunderstanding about the concept and scope of article 16, namely, that article 16 is limited to preservation of computer data held by communication service operators. For all of the aforementioned reasons, we consider it useful to make some preliminary observations about the nature and the scope of application of article 16.

Firstly, it should be noted that nothing in the text of the Convention or its Explanatory report is meant to limit the application of article 16 only to data held by communication service operators. While it might be true that the Explanatory report recognizes the limitations of preservation order and therefore stipulates that such an order might be useful "where the custodian of the data is trustworthy, such as [in the case of] a reputable business", and that in other cases data might be preserved by different methods ("search or similarly access and seize or similarly secure the data"), there is nothing to suggest that preservation order could not, if considered appropriate in the particular case, be used in order to secure data held by any natural or legal person.[18]

The other question, which is also relevant in the context of this Report, concerns the method of implementation of article 16 into national legislations. In this context, it was concluded at the T-CY meeting in December 2012 that some Parties use *"search and seizure, production orders or similar powers to preserve electronic evidence. These approaches are valid in the meaning of the Budapest Convention, if such powers permit to secure electronic evidence in relation to any crime and any legal or physical person holding data in an expedited manner. The Budapest Convention does not necessarily require that Parties establish a specific provision in their criminal procedure law…*".

This question is of particular relevance for this Report since none of the surveyed countries implemented article 16 via specific provisions. However, while it is true that the Convention does not mandate that Parties to implement preservation measure as a specific order, we believe that such an approach is by far a better option. In this context, it should also be taken into account that the order to preserve data is, in comparison to the search and seizure measure, far less, if at all, invasive to the rights and interests of person to whom it is directed. The Explanatory report also follows this approach when it states (although in relation to Production order) that "instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations."

Finally, there is a question of what are the appropriate conditions and safeguards that should be used in relation with article 16. It can be concluded that this also depends on the method of implementation of article 16. If the preservation order is given effect via production order or search and seizure, then conditions and safeguards used for those measures should be applicable. On the other hand, in case of implementation of a preservation order as a standalone measure, specific conditions and safeguards, which are "appropriate in view of the nature of the procedure or power", should be used. One of these conditions is provided in article 16/3 of the Convention, according to which preservation order should be effective "for a period of time as long as necessary, up to a maximum of ninety days". Another issue relevant in the context of safeguards connected with article 16 is the question of relevant authority to issue such orders. Since most of the Parties to the Convention still did not implement article 16, or did not implemented in fully, it is not possible to argue with certainty what conditions should be used in this regard. It appears, however, that an order to preserve data would not necessarily have to be based on a court's

[18] See T-CY Assessment report regarding „Implementation of the preservation provisions of the Budapest Convention on Cybercrime", para. 8: *"Article 16 is a provisional measure that allows the authorities to order the immediate preservation of data already stored on a computer system. This may include traffic but also content data, and it may include data held by a service provider, but also by any other physical or legal person."*

decision.[19] In our view, this approach could not be objected, due to the relatively small impact of the measure on the interests of the person to whom the order is directed.

### 1.5.5 Expedited preservation and partial disclosure of traffic data (Article 17)

Article 16 provides for a general legal framework necessary to enable preservation of computer data in general. This data includes also so called "traffic data". When it comes to preservation of traffic data, rules established in Article 16 should be used in conjunction with Article 17, which provides for some measures specific to traffic data. The purpose of Article 17 is well explained by the Explanatory Report:

> 166. Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who, for example, have distributed child pornography, distributed fraudulent misrepresentations as part of a fraudulent scheme, distributed computer viruses, attempted or successfully accessed illegally computer systems, or transmitted communications to a computer system that have interfered either with data in the system or with the proper functioning of the system. However, this data is frequently stored for only short periods of time, as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data. Therefore, it is important that preservation measures be undertaken to secure the integrity of this data (see discussion related to preservation, above).
>
> 167. Often more than one service provider may be involved in the transmission of a communication. Each service provider may possess some traffic data related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. Sometimes traffic data, or at least some types of traffic data, are shared among the service providers involved in the transmission of the communication for commercial, security, or technical purposes. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.

In order to give effect to the aforementioned goals, Article 17 requires that Parties to the Convention adopt legislative and other measures which may be necessary to: (a) ensure that 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.

### 1.5.6 Production order (Article 18)

According to Article 18, Parties to the Convention must adopt "such legislative and other measures as may be necessary to empower its competent authorities" to (a) order "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) order a "service provider

[19] For some examples on implementation of article 16 see report on "Implementation of the preservation provisions of the Budapest Convention on Cybercrime".

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."[20]

What conditions and safeguards should be used in relation to production order? In the context of conditions and safeguards mentioned in the Explanatory Report, [21] we believe that the production orders should in particular be subject to judicial supervision (or supervision by other independent body), and that the application of this measure in concrete cases should always be based on specific grounds established by the law.

### 1.5.7 Search and seizure of stored computer data (Article 19)

Article 19 of the Convention was written with the aim of providing specific legal framework necessary to efficiently conduct search and seizure measures in relation to computer systems and data. According to the Explanatory Report, the drafters of the Convention recognized the fact that there are many similarities between the search and seizure of tangible objects and the same measures applied in the context of computer systems and data. However, it was also considered that:

> "…additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record. The physical medium on which the intangible data is stored (e.g., the computer hard-drive or a diskette) must be seized and taken away, or a copy of the data must be made in either tangible form (e.g., computer print-out) or intangible form, on a physical medium (e.g., diskette), before the tangible medium containing the copy can be seized and taken away. In the latter two situations, where such copies of the data are made, a copy of the data remains in the computer system or storage device. Domestic law should provide for a power to make such copies. Third, due to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. It could be stored in an associated data storage device that is connected directly to the computer, or connected to the computer indirectly through communication systems, such as the Internet. This may or may not require new laws to permit an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use traditional search powers in a more co-ordinated and expeditious manner at both locations."[22]

For these reasons, Article 19 of the Convention contains a series of requirements which are specific for computer-related search and seizure and which the Parties should therefore observe.
In this report, we will analyse the manner and level of implementation of Article 19 in the national legislations of the project countries. In that context, special attention will be given to the requirements arising under Article 15. Applied in the context of Article 19, Article 15, in our view, mandates in particular that there is (1) judicial (or other independent) supervisions over the application of the measure, that (2) its use is justified in accordance with the grounds stipulated in

[20] For the purposes of the Convention, subscriber information are defined as „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 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.

[21] See paragraph 147 of the Explanatory Report.

[22] Explanatory report, para. 187.

the law and that (3) other safeguards, in particular those exempting certain persons or places from the application of the measure are used.

### 1.5.8 Interception of content data (Article 21)

In addition to the aforementioned general requirements arising under Article 15, it is possible to identify some safeguards which are used specifically in relation to Article 21.

According to the Explanatory Report:

> 212. With respect to the real-time interception of content data, the law often prescribes that the measure is only available in relation to the investigation of serious offences or categories of serious offences. These offences are identified in domestic law as serious for this purpose often by being named in a list of applicable offences or by being included in this category by reference to a certain maximum sentence of incarceration that is applicable to the offence. Therefore, with respect to the interception of content data, Article 21 specifically provides that Parties are only required to establish the measure 'in relation to a range of serious offences to be determined by domestic law'.

The abovementioned limitation of the scope of Article 21 is an explicit example of the application of proportionality principle and should be followed by all the Parties to the Convention.

In addition, we would also like to draw the attention to some of the standards established in the case-law of the ECtHR. In Malone v. UK, the court explained that:

> 67. … the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention …. The phrase thus implies - and this follows from the object and purpose of Article 8 … that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 …. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident…. Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.

In Kruslin v. France,[23] the court held that:

> 33. Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.

[23] Application no. 11801/85.

In Klass v. Germany, the court argued that:

> 42. The cardinal issue arising under Article 8 (art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.

### 1.5.9 Real-time collection of traffic data (Article 20)

According to the Explanatory Report:

> 211. In some States existing legislation makes no distinction between the collection of traffic data and the interception of content data, either because no distinction has been made in the law regarding differences in privacy interests or the technological collection techniques for both measures are very similar. Thus, the legal prerequisites required to authorise the undertaking of the measures, and the offences in respect of which the measures can be employed, are the same. …

In the same context, Article 14/3 of the Convention provides that:

> 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.

The following chapters discuss the conditions and safeguards established in each country regarding the powers under Articles 16 to 21 Budapest Convention.

# 2 Armenia

## 2.1 Available documents and other sources

This part of the report (regarding Armenia) is based on (1) the Armenian reply to the Questionnaire sent to the countries of the Eastern Partnership (hereinafter: AR Reply), (2) Excerpts from the Armenian Code on Criminal Procedure (hereinafter: ArCPC), provided in the AR Reply, (3) Excerpts from Armenian Criminal Code (hereinafter: ArCC), provided in the AR Reply, (4) Excerpts from Armenian Law on Operative-Search Activity (hereinafter: ArLOSA), provided in the AR Reply, and (5) Roundtable discussion on Article 15 of the Budapest Convention (Strasbourg, France, 7 December 2012).

## 2.2 Expedited preservation of stored computer data

Armenia did not implement Article 16 as a standalone measure. As regards the possibility to use production order or search and seizure to give effect to Article 16, it was noted that such an option is in theory possible, but it has not yet been used in practice.

## 2.3 Expedited preservation and partial disclosure of traffic data

Article 17 of the Convention is not implemented in Armenian legislation. Hypothetically, it is possible to argue that production order and/or search and seizure could be used. However, it was submitted that these options were not tested in practice.

## 2.4 Production order

In the domestic legislation of Armenia there are no specific provisions with the scope and purpose corresponding to Article 18. Instead, it is evident that search and seizure is the default measure used to obtain stored computer data in someone's possession or control (see below in 2.4).

However, even if search and seizure measure can be effectively used to obtain stored computer data by Armenian authorities, its use still does not amount to valid implementation of Article 18. In this context, it should be noted that Article 18 is different than Article 16, in the sense that the while it might be possible for the Parties to implement preservation order via production order or search and seizure, there surely is not an option to give effect to production order by search and seizure measure. The core purpose of Article 18 is to enable relevant authorities to use "alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations".[24] In order to give effect to Section 2, Parties should implement all of the measures defined therein, and they certainly must implement all of the measures defined in articles 18-21. If this was not the case than all of the six measure established in the Convention could, in national legislations, collapse into the measures of search and seizure and interception of communications. In that case, however, the purpose of the Section 2, which seeks to provide gradual system of procedural powers with different levels of intrusiveness, could never be achieved.

In addition to general rules on search and seizure, which are discussed below, it was submitted in AR Reply that police and NSS (National Security Service) are competent to order and withdraw computer and subscriber data in accordance with the ArLOSA, on the basis of a court order. Also, it was stated in the AR Reply that Article 49 of Law on Electronic Communications obliges service providers to keep (confidentially) some information about their subscribers. We were not, however, provided with the text of these provisions. In any case, they should be reviewed in the light of Article 19.

[24] Explanatory Report, paragraph 170.

## 2.5 Search and seizure of stored computer data

There are no provisions in the ArCPC which would provide for a specific, computer-related search and seizure measures. Therefore, traditional powers of search and seizure of tangible objects are used to give effect to the Article 19 in Armenia.

General requirement justifying application of the search measure is that there are "sufficient grounds to suspect that in some premises or in some other place or in possession of some person, there are instruments of crime, articles and valuables acquired by criminal way, as well as other items or documents, which can be significant for the case" (ArCPC, article 225). It was confirmed during the discussions for the preparation of this report that the term "document" in ArCPC can be interpreted broadly enough to cover computer data. From the formal viewpoint, search is executed on the basis of a court order (ArCPC, 225/3).

As regards the situation envisioned in Article 19/2, it should be noted that no specific provisions applicable to this situation can be found in the ArCPC. Therefore, it follows that if the data which are sought are stored in another computer system, which is held in a place not covered by the original court order, a new order would be required.

As regards Article 19/3, applicable provision in the ArCPC is article 226, which enables authorities to seize "articles and documents significant for the case", provided it is known where and in whose possession they can be found. In addition to this authority article 225/1 of the ArCPC enables investigators to seize ("take") "instruments of crime, articles and valuables acquired by criminal way, as well as other items or documents, which can be significant for the case" in the course of conducting a search measure. Specific options for conducting a search measure, enumerated in Article 19/3, are not regulated in ArCPC. However, it was confirmed during the Roundtable discussion that authorities performing the seizure measure are able to execute it in different manners, on the basis of circumstances in every particular case.

Article 19/4 is not implemented.

As regards the application of Article 15, it can generally be concluded that Armenian legislation provides adequate safeguards and conditions which limit the application of search and seizure measures. According to the information submitted in the AR Reply and confirmed during the discussions, it appears that the following conditions and/or safeguards (except those already mentioned – grounds to apply the measure and the requirement of a court order) are used in relation to search and seizure measure:

First of all, it has to be noted that an open criminal case is absolute prerequisite for the execution of a search and/or seizure measure. Provided that this requirement is satisfied, the following principles apply:

- Search can be conducted only on the basis of the court order, when there are sufficient grounds to suspect that objects significant for the case can be found in some premises or in some other place or in possession of some person (ArCPC, art. 225/1,3)
- Attesting witnesses, as well as of some other persons25 in specific circumstances, should be present when conducting a search and/or seizure (ArCPC, art. 227)
- Prior to conducting search and /or seizure, investigator should present the search warrant to the person against whom the measure is directed (ArCPC, art. 228/1)
- Investigators are under the obligation to keep confidential facts established during search / seizure, as well as details regarding private life of the searched persons (ArCPC, art. 228/4)
- A search protocol has to be prepared and given to relevant persons (ArCPC, art. 231).

[25] Members of the family / representatives of the apartment maintenance / local administration / representatives of enterprises, institutions, organizations, military units. See ArCPC art. 227

In addition to the aforementioned conditions, which are defined by the Criminal Procedure Code, there are several provisions in the Armenian Criminal Code which provide for criminal sanctions in the cases of illegal collecting, keeping, use and dissemination of information pertaining to personal or family life (art. 144), abuse of official authority (art. 308) and divulging the data of inquiry or investigation (art. 342).

## 2.6 Real-time collection of traffic data and interception of content data

In the Armenian legislation, no distinction is made between the real-time collection of traffic data and real-time interception of content data: the same set of legal rules and conditions / safeguards is used in relation to both of these measures. An execution of measures which correspond to articles 20 and 21 of the Convention is considered to be a so-called "operative-search" activity. These actions are covered by a combination of provision contained in the ArCPC and ArLOSA.

In this regard, the ArCPC provides for general legal conditions for the execution of these measures, while the ArLOSA's subject-matter is institutional and procedural framework for their implementation. As regards ArCPC, reference was made (in AR Reply) to its articles 239 and 241, which provide for "monitoring of correspondence, mail, telegrams and other communications" and "supervision over conversation". On the other hand, ArLOSA defines, in its Article 26, the general measure of wiretapping. The translated text of this article reads as follows:

**Article 26. Wire tapping**

Wire tapping is the secret control over the phone conversations, including internet conversations and electronic communications by means of special and other technical devices, which means:

1) in case of fixed phone network:

a. recording of phone conversation or recording of its content in other form;

b. identification of the phone number;

c. collection and (or) identification of the individual date of the subscriber of the given phone number, location and move of the interlocutors at the beginning and during the phone conversation;

d. in case of call divert or transfer identification of the phone number on which the call has been transferred;

2) in case of mobile phone network:

a. recording of the phone conversation, including sms and voice mails or other type recording of their content;

b. date of beginning and end the phone conversation, phone number, individual date of the subscriber of the given phone number, collection and (or) identification of necessary information about the location and move of the interlocutors at the beginning and during the phone conversation;

3) in case of internet communication, including in case of internet phone conversations and e-messages forwarded via internet – recording of the communication or otherwise recording of its content, as well as the data with the help of which one can determine:

a. geographical location, day, hour and duration of connecting to internet and getting out of it, including IP address;

b. name and user ID of internet user or subscriber;

c. the phone number with which he/she connects to the general phone network, internet address, name of the persons having received internet phone call or each detail on facts, cases and circumstances about that person in a form that enables or may enable to identify him/her.

## 2.7 Real-time collection of traffic data

As regards measure corresponding to article 20 of the Convention, ArLOSA does not define the term "traffic data". However, it follows from the text of article 26 of ArLOSA that it is possible to collect certain categories of data which qualify as traffic data in the terms of the Convention using general wiretapping procedures. Provisions contained in paragraphs 1/b-d, 2/b and 3/a-c, cited above, refer to the collection of other data besides content of the communication under surveillance.

## 2.8 Interception of content data

The legal basis is Articles 239 and 241 of the ArCPC, which read as follows:

Article 239. Monitoring of correspondence, mail, telegrams and other communications

When there are sufficient grounds to believe that there is probatory value data in the mail or other correspondence, mail, telegrams and other communications (referred to below as correspondence) sent by the suspect or the accused or to them by other persons, the investigator can make a grounded decision to impose monitoring on the correspondence of these people.

The decision must indicate the name of the post office which is responsible for withholding of the correspondence, the name(s), surname(s) of the person(s) whose correspondence…

Article 241. Supervision over conversation

If there are sufficient grounds to suspect that the telephone conversations of the suspect or the accused or the conversations conducted by other means of communication can contain significant information for the case, the court makes a decision to permit the supervision and recording of these conversations.

The investigator makes a grounded decision on initiating an application to the court, which indicates the criminal case and grounds on which the appropriate investigatory actions must be taken, the surnames and names of the persons whose conversations are subject to supervision, the supervision period, institution which is instructed to conduct the technical implementation of supervision and recording. The decree is forwarded to the court.

In case of approval by the judge, the conversation supervision and recording decision is forwarded by the investigator to the appropriate institution for implementation.

Conversation supervision and recording can be limited by no longer than six months. They are lifted when the necessity for them is over, but in any case, no later than the end of the preliminary investigation.

The investigator is entitled to demand the record at any time for examination and listening within the established period. The record is handed to the investigator in the sealed form with an accompanying letter which must indicate the time of beginning and

end of the record of conversations, and necessary technical description of used devices.

Examination and listening of records by the investigator is done in the presence of attesting witnesses, and when necessary, experts, about which a protocol is written.

From a procedural point of view, the provisions of article 26 of the ArLOSA, cited above, are applicable.

## 2.9 Conditions and safeguards

As was stated above, the legal framework for real-time collection of traffic data and interception of content data is the same in Armenia; therefore, the same set of conditions and safeguards is applicable for both of the measures corresponding to article 20 and 21 of the Convention.

As a general rule, it was underlined during the roundtable discussion that an open criminal case is the basic precondition for the application of these measures. In addition, it was emphasized that the measure of wiretapping can be used only for a limited catalogue of criminal offences, although we were not provided with the list of those crimes.

Operative-search activities discussed in this chapter (2.5) can only be carried out on a basis of a court order, which is granted upon a motion of a body in charge of the investigation. The procedure for conducting the aforementioned measures is extensively defined in article 32 and the following articles of the ArLOSA, which provides for several conditions and safeguards.

As a basic rule, a court order is required in order to implement any of the measures defined in article 26. However, in certain limited circumstances,[26] it is possible to start executing the measure even without a court order; such an order then must be submitted within 48 hours. Failure to do so will result in immediate termination of the measure and all the previously acquired information shall be deleted. In addition, article 32/3 of the ArLOSA mandates that the head of the body performing the measure of wiretapping immediately informs the President of the Republic about any such case (where the appropriate court order was not submitted within the 48 hours).
In addition, Article 40/2 mandates that detailed minutes of the measure be taken by the body performing them.[27]

Article 40/4 provides that information which is not envisaged by the decision on conducting the measure, about the person in regard of whom the measure was performed, shall not be considered as evidence and will be destroyed, except when:

[26] Article 32/2 of the ArLOSA: "when the delay of conducting the operational and search measures may lead to commitment of terrorism or events or actions threatening the state, military or environmental security of the Republic of Armenia…"

[27] Article 40/2 reads as follows: "The minutes of the operational and search measures are taken by the official conducting them. The minutes shall contain the place, time, circumstances of conducting the operational and search measure; the names, surnames, positions of the operational staff conducting the operational and search measure and other participants of the operational and search measure, as well as the names and surnames of the persons (or their legitimate representatives), in regard of whom all the actions undertaken during the operational and search measure are applied to in the sequence like those have been committed; applied scientific-technical methods and measures, as well as the information, materials and documents acquired as a result of that measure. The minutes are signed by the official(s) having conducted the operational and search measure."

1) The bodies performing operational and search activities have acted in good faith and

2) The information received contains information about grave and specially grave crime or such crime being prepared and

3) For the acquisition of that information this law permits to conduct such operational and search measure.

Beside aforementioned conditions and safeguards, which define conditions and safeguards used in individual cases, article 32/4 of the ArLOSA establishes a system of presidential supervision of measures of secret surveillance. According to this provision, the head of the body which performs the measures of wiretapping must inform the President of the Republic, once a year, about:

1) overall number of motions submitted to the Service to perform operational and search measures envisaged by this article;

2) number of motions that were brought without court decision extract and no extract submitted in the aftermath;

3) number of the motions that were brought without court decision extract and the court in the aftermath did not permit with its decision the conduct of such operational and search measures.

## 2.10 Summary

| Article | Situation in Armenian legislation | Recommendation |
|---|---|---|
| 16 | Not implemented. | Armenia might wish to consider the implementation of a specific preservation order in the ArCPC. Scope and purpose of such orders are discussed above (1.5.4.). |
| 17 | Not implemented. | Armenia might wish to consider the implementation of specific provisions regulating preservation of traffic data, in accordance with the scope and purpose of Articles 16 and 17. |
| 18 | Not implemented in line with Article 18, as a specific measure. Seizure procedure is used to access stored data. | Article 18 should be implemented as a specific order, different from the seizure procedure, and under its own set of conditions and safeguards.<br>Provisions of the ArLOSA and the Law on Electronic Communications should be reviewed in the light of Article 18. |
| 19 | No specific provisions on computer-related search and seizure; "traditional" rules on search and seizure are used.<br><br>Conditions and safeguards used are described above (2.5). | Armenia might wish to consider the implementation of specific provisions providing legal framework for computer-related search and seizure.<br>Situation envisioned in Article 19/2 should be addressed in specific provisions in ArCPC. Different options of seizing and similarly securing computer data, enumerated in Article 19/3, should be transposed in ArCPC.<br>Article 19/4 should be implemented in ArCPC, with appropriate conditions and safeguards.<br>Existing conditions and safeguards, mentioned above (2.5) should be kept in place. |
| 20 | Partly covered by the provisions of ArCPC and ArLOSA's rules on wiretapping. | See below. |

| | | |
|---|---|---|
| 21 | Partly covered by the provisions of ArCPC and ArLOSA's rules on wiretapping. | Armenia might wish to review the ArCPC in the light of Article 20, with the aim of amending provisions of articles 239 and 241. It is clear from the text of these articles that they are not best suited for the execution of the measures defined in Articles 20 and 21.<br><br>We recommend that specific legal provisions, implementing directly Articles 20 and 21, be introduced in ArCPC. Conditions and safeguards used in relation to these measures should be in line with the requirement of the Convention.<br>In our view, it would be necessary to review the scope of ArCPC and ArLOSA with the aim of coordinating their rules. In this context, we believe that most of the conditions and safeguards should be provided in ArCPC. |

# 3 Azerbaijan

## 3.1 Available documents and other sources

This part of the Report (regarding Azerbaijan) is based on (1) Azeri reply to the Questionnaire sent to the countries of the Eastern Partnership (hereinafter: AZ Reply); (2) Code on Criminal Procedure (hereinafter: AzCPC),[28] (3) Detective-Search Activity Act (hereinafter: AzDSAA)[29] and (4) Law on Intelligence and Counter-Intelligence Activities (AzICIA) of Azerbaijan;[30] as well as (5) information collected during the Roundtable discussion on Article 15 of the Budapest Convention (Strasbourg, France, 7 December 2012).

## 3.2 General remarks regarding the structure of the Azeri legislation with respect to Section 2 of the Convention

AzCPC is the main source of Azeri legislation relevant in the context of implementation of Section 2. In addition, some aspects of the measures discussed in this report are also covered by AzDSAA. In general, AzCPC gives effect to the Section 2 Budapest Convention through a series of provisions which regulate the collection of evidence in general and some of the "investigative procedures", in particular. In short, it could be said that articles 16, 17 and 18 are (partially) implemented via general rules regarding collection of information for the purposes of establishment of evidence. Article 19 of the Convention is covered by a series of provisions which regulate search and seizure (as "traditional" measures, since there are no rules on specific computer-related search and seizure), and articles 20 and 21 are covered by rules on interception of communications. The distinction between norms which give effect to articles 16-18, on one side, and those which cover articles 19-21, on the other, is also based on the fact that the former ones are based on the concept of voluntary submission of information, and the latter are recognized as investigative procedures which are (in principle) carried out "by force" (involuntarily).

## 3.3 Expedited preservation of stored computer data

Azerbaijan did not implement Article 16 as a standalone measure. In order to achieve the purpose of this article production order is used, and search and seizure is an available alternative.

During the discussions for the preparation of this report, it was confirmed that rules on production of documents, discussed below (3.4), are used in practice in order to gain access to stored computer data. Generally speaking, these provisions can be used in relation to any person or entity that is in possession of any type of specific computer data. On the other hand, it should be noted that the measure defined in AzCPC 143.2 can only be applied during the process of collecting evidence, after a formal investigation has been initiated. While the application of this condition could theoretically bring into the question the expedient nature of the measure, it was confirmed during the discussions for the preparation of this report that Azeri authorities are able to gain access to stored computer data in a sufficiently expedient manner. The same goes for the issue of possible non-compliance with the request to produce data. According to the information available to us, holders of stored computer data in general provide an adequate level of support to the authorities, and in cases of possible non-compliance the use of search and seizure measure is available as an alternative.

[28] Text of the AzCPC was provided by the Council of Europe's Secretariat. It was adopted on 14 July 2000; no subsequent amendments were indicated in the document.

[29] Available at http://www.mia.gov.az/index.php?/en/content/29012/ (21.02.2013).

[30] Relevant excerpts from this act were translated and provided to us by Mr. Samir Mukhtarzade.

## 3.4 Expedited preservation and partial disclosure of traffic data

Preservation and disclosure of traffic data is regulated in a sort of *sui generis* manner in Azerbaijan. In general, there is no legal obligation for service providers to retain traffic data. However, on the basis of the Law on Intelligence and Counter-Intelligence Activities (AzICIA), communication operators are required to establish an "appropriate level of cooperation with Azeri authorities", thereby enabling and assisting in the execution of some of the procedural measures in criminal cases.

The ranslated text of the relevant provisions of AzICIA reads as follows:

> **Article 17 Information support to the subjects of intelligence and counter-intelligence activity**
>
> 17.4 Irrespective of the organizational-legal form and the form of ownership, all telecommunications agencies operating on territory of Azerbaijan are obliged to create conditions for carrying out intelligence and counter-intelligence actions in an order, established by the legislation, for that purpose to supply corresponding communication networks with additional equipment according to the conditions defined by corresponding executive power authority, to solve organizational issues and to keep in secrecy the methods used while carrying out of these actions.
>
> **Article 39 Interrelation between operators, providers and bodies implementing search activity**
>
> 39.1 Operators, providers must promote in proper legal manner implementation of search actions, supply telecommunication nets with extra technical devices according to terms set by corresponding executive power body for this goal, solve organizational issues and keep methods used in implementation of these actions as secret.
>
> 39.2 Operator, provider bears responsibility for violation of these requirements in proper legal manner.

On the basis of these provisions, Azeri authorities have concluded a number of memoranda of understanding with ISP's and other communication operators, specifying the details of their cooperation. Among other obligations, operators are required to enable Azeri authorities to access certain categories of data which operators retain for business purposes, or otherwise on their own motion. Some of these data qualify as traffic data in the terms of the Convention. According to available information, different providers retain various types of data about communications, for different periods of time (3 – 24 months), in accordance with their own policies and technical capabilities.

In order to gain access to data about communications, stored by the service providers, it is necessary to produce a court order, which is issued upon a motion of a prosecutor. During the discussions it was confirmed that in practice Azeri authorities do not experience significant problems with obtaining data from communication operators. In addition, it was underlined that in cases of urgency it is possible to gain access to traffic data in an expedient manner, and that it would be possible to establish an appropriate level of cooperation in cases when multiple service providers are involved in the communication chain.

## 3.5 Production order

The general legal framework for the production of data in the AzCPC is established by its article 143 which is read in conjunction with article 135, discussed above (3.2. and 3.3). As was previously explained, these provisions enable Azeri authorities to request the production of any type of stored computer data. However, article 143.2 of the AzCPC provides only the possibility of

voluntary production of data and as such does not have to be based on the court order. In the situation when the production of data is refused, the only workable alternative is search and seizure measure.

In addition, article 18 of the Convention contains a specific power to order the production of "subscriber information", which is defined in paragraph 2 of that article. In this context, it should be noted that Azeri legislation does not contain the definition of the term "subscriber information". However, it was confirmed that in practice service providers have in their possession information which fall into that category, and their production is subject to the same rules as for the computer data in general.

## 3.6 Search and seizure of stored computer data

There are no specific provisions on search and seizure of computer systems in Azeri legislation; therefore, the legal framework for traditional search and seizure is applicable.

In general, search is defined as one of the methods of evidence collection (AzCPC, 143.1). In order for a search measure to be executed, it is necessary that a formal investigation is open. As a general rule, search and seizure can be conducted on the basis of a court order (AzCPC, 243.1.), which is issued upon a motion of a prosecutor, following reasoned request of an investigator (AzCPC, 243.1.). In certain, highly limited circumstances, it is possible to conduct a search without the court order (AzCPC 243.3).[31]

According to AzCPC, a search order can be issued when "available evidence or material discovered in a search operation give rise to a suspicion that a residential, service or industrial building or other place contains, or certain persons are in possession of, objects of potential significance to a case".

From the procedural viewpoint, a search is executed by an investigator in the presence of two attesting witnesses, the person against whom the search and seizure are being conducted or adult members of his family, or those who represent his legal interests. Where necessary, an interpreter or specialist may participate in the conduct of the search or seizure.

Detailed rules regarding procedure for the execution of these measures are provided in article 245 of the AzCPC, which reads as follows:

[31] AzCPC: "243.3. In circumstances which admit no delay, the investigator may conduct a search or seizure without court permission only if there is precise information indicating that:
243.3.1. objects or documents concealed in a residential building constitute proof of the commission of an offence or of preparations for the commission of an offence against a person or the state;
243.3.2. a person who has prepared or committed an offence against a person or the state or a person who has escaped from a remand facility or prison is hiding in a residential building;
243.3.3. there is a human corpse (or parts of a corpse) in the building;
243.3.4. there is a real danger to someone's life or health in the building.
243.4. In the circumstances provided for in Article 243.3 of this Code, the investigator shall give a reasoned decision to conduct a search or seizure. The investigator's decision shall be drawn up in accordance with the requirements of Article 243.2 of this Code and shall give due consideration to the need to conduct the search and seizure without court permission and the reasons why it cannot be delayed."

**Article 245. Rules governing searches and seizures**

245.1. An investigator shall be entitled to enter a residential or other building on the basis of the court decision concerning the search or seizure.

245.2. Before conducting the search or seizure, the investigator shall acquaint the person concerned with the decision.

245.3. The investigator shall be entitled to conduct the search or seizure using photography, video, film or other recording techniques.

245.4. The investigator shall take measures to prevent the dissemination of information about the circumstances of the search or seizure, its results and any information concerning the private life of the person concerned.

245.5. The investigator may prohibit those present in the place where the search or seizure is conducted from leaving the premises or speaking to each other or with other persons before the end of the search or seizure operation.

245.6. On making a seizure, the investigator shall, after pronouncing the decision, propose that the objects or documents to be seized be surrendered voluntarily and, in the event of refusal, shall impound them by force.

245.7. On conducting a search, the investigator shall, after pronouncing the decision, propose that the objects or documents to be seized be given up voluntarily and that the wanted person's hiding place be revealed. If the objects or documents are surrendered or the person's hiding place is revealed voluntarily, this shall be noted in the record. Failure to surrender the objects or documents being searched for, in whole or in part, or to reveal the hiding place of the wanted person, shall result in the search being conducted.

245.8. During a search or seizure, all objects and documents shall be presented to the participants in the investigative procedure and their quantity, size, weight, material and other special features shall be specified as part of a detailed description. The objects and documents shall be packed and, if necessary, sealed by the investigator.

245.9. If, during the conduct of a search or seizure, the owners refuse to open closed buildings or store-rooms, the investigator shall have the right to open these.

…

The third paragraph of article 19 of the Convention, which stipulates that national authorities should have four separate powers (methods) of seizing data, is not implemented in Azeri legislation. However, it was submitted that in practice there would be no legal obstacles to utilizing any of the measures defined in article 19/3; although, usually only the first two options are being used.

Similarly, the fourth paragraph of article 19 of the Convention also does not have a corresponding provision in the Azeri law. In this respect, it was submitted that the standard course of action is to enable an examination of computer data using some of the available technical (forensic) measures.

## 3.7 Real-time collection of traffic data and interception of content data

In general, Azeri legislation does not differentiate between real time collection of traffic data and content data; therefore, it would appear that the same set of rules is applicable in both cases. However, it was submitted during the discussions for the preparation of this report that Azeri authorities do not apply measure defined in article 20 of the Convention in practice. In any case,

should the real-time collection of traffic data be executed in Azerbaijan, it would have to follow the legal framework established for interception of content data, which we discuss below.

Article 21 of the Convention is implemented in Azeri legislation in an article titled "Interception of conversations held by telephone and other devices, of information sent by communication media and other technical means, and of other information", which is one of the "investigative procedures" enumerated in AzCPC 177.3, and is regulated in more detail in article 259 of the AzCPC, which reads as follows:

> **Article 259. Interception of conversations held by telephone and other devices, of information sent by communication media and other technical means, and of other information**
>
> 259.1. Interception of conversations held by telephone and other devices and of information sent by communication media and other technical means shall as a rule be carried out on the basis of a court decision. Where there are sufficient grounds to suppose that information of significance to the criminal case is included among information sent or received by the suspect or the accused, the court shall, on the basis of a reasoned request by the investigator and appropriate submissions by the prosecutor in charge of the procedural aspects of the investigation, authorize the interception of conversations held by telephone or other devices, information sent by communication media or other technical means, or other information. Interception of such conversations and information shall be carried out in accordance with Article 177.2-177.5 of this Code.
>
> 259.2. Interception of conversations held by telephone and other devices or of information sent by communication media or other technical means shall not continue for longer than 6 (six) months.
>
> 259.3. Interception of information which comprises personal, family, state, commercial or professional secrets, including information about financial transactions, the situation of bank accounts and the payment of taxes, may be carried out only on the basis of a court decision.
>
> 259.4. The decision authorising the interception of conversations held by telephone and other devices, of information sent by communication media or other technical means, or of other information shall state the following:
>
> 259.4.1. the date, time and place of the decision;
>
> 259.4.2. the family name, first name, father's name and title of the person who made the decision;
>
> 259.4.3. the objective grounds and reasons for intercepting the relevant conversations and information;
>
> 259.4.4. the family name, first name, father's name and exact address of the person(s) whose information or conversations are to be intercepted;
>
> 259.4.5. the exact type(s) of conversation or information to be intercepted;
>
> 259.4.6. the name of the administration assigned the duty of intercepting the conversations or information;
>
> 259.4.7. the period for which interception of the conversations and information is to be carried out.

> 259.5. Conversations held by telephone and other devices, information sent by communication media or by other technical means and other information shall be intercepted by those authorised to do so, on the basis of the relevant decision. The intercepted conversations and information shall be transcribed on paper or copied on magnetic devices, confirmed by the signature of the person who intercepted them and given to the investigator. A summary record of the interception of the conversations and information related to the case shall be drawn up and added to the case file. Intercepted information not related to the case shall be immediately destroyed.

In addition, the matter of article 21 of the Convention is also covered by article 10 of the AzDSAA, which provides for a list of detective-search actions and includes, *inter alia*,

> 3) tapping telephone conversations;
>
> 4) examination of postal, telegraphic and other correspondence;

From the combined interpretation of the AzCPC and AzDSAA, it follows that the court order is the main condition for the application of measures of interception of content. According to AzCPC 177.4.4., it is possible to apply the measure of interception of communications (AzCPC 259) when "evidence of serious or very serious offences against the individual or central government must be established without delay". In that case, the investigator is under the obligation to:

> 443.2.1. within 24 hours, inform the court exercising judicial supervision and the prosecutor in charge of the procedural aspects of the investigation of the investigative procedure conducted;
>
> 443.2.2. within 48 hours, submit the material relating to this investigative procedure to the court exercising judicial supervision and the prosecutor in charge of the procedural aspects of the investigation in order that they may verify the legality of the investigative procedure conducted.

Some of the safeguards limiting the possibility of intercepting communications are also provided in AzDSAA. According to this law,

> Detective-search measures in respect of confidentiality of information protected by legislation and transmitted by correspondence, telephone, post-telegraph and other means of communication… shall be allowed if there are sufficient grounds to believe that the measures … will produce information to serve as evidence in criminal proceedings and location. (AzDSAA, 13.I.)

In addition, it should be noted that article 10.III. of the AzDSAA stipulates that the aforementioned actions can only be executed when it is impossible to achieve the goals of the law by other (less invasive) means. The maximum duration of interception is set at six months.

## 3.8 Summary

In general, Azeri legislation in the field of criminal procedural law is regulated in extreme detail. This is, however, not the case with the provisions which seek to give effect to Section 2 of the Convention. The main reason for this is obviously the fact that AzCPC was adopted on 15 July 2000, before the Convention was even signed. Therefore, while the AzCPC can in some aspects be seen as over-normative, it notably lacks any mention of computer systems or data, traffic data, subscriber information or other terms which are specific subject-matter of the Convention.

| Article | Situation in the Azeri legislation | Recommendation |
|---|---|---|
| 16 | Not implemented as a specific measure; rules on production of documents are used. | Azerbaijan might wish to consider the implementation of a specific preservation order in the AzCPC. Scope and purpose of such orders are discussed above (1.5.4.) Preservation measure could follow its own set of conditions and safeguards and should not necessarily be based on the condition of formal investigation being opened. |
| 17 | Not implemented as a specific measure; informal cooperation with service providers enables the preservation of traffic data in line with the purpose of Article 17. | With regard to Article 17, Azerbaijan is in line with the Convention. |
| 18 | Article 143 of the AzCPC enables voluntary transfer of documents; alternatively, it is necessary to use search and seizure. | Azerbaijan might wish to consider the implementation of a specific production order in the AzCPC. Such an order should be drafted in line with Article 18, differentiate between production of computer data in general and subscriber information and follow its own set of conditions and safeguards. |
| 19 | No specific provisions on computer-related search and seizure; "traditional" rules on search and seizure are used.<br><br>Conditions and safeguards used are described above (3.5). | Azerbaijan might wish to consider the implementation of specific provisions providing legal framework for computer-related search and seizure.<br><br>Situation envisioned in Article 19/2 should be addressed in specific provisions in ArCPC.<br><br>Different options of seizing and similarly securing computer data, enumerated in Article 19/3, should be transposed in ArCPC.<br><br>Article 19/4 should be implemented in ArCPC, with appropriate conditions and safeguards.<br><br>Existing conditions and safeguards, mentioned above (3.5) should be kept in place. |
| 20 | No specific provisions in AzCPC. It was submitted that the measure is not applied in practice. | Azerbaijan might wish to consider the implementation of specific provisions providing for real-time collection of traffic data. |
| 21 | Implemented by a combination of provisions in AzCPC and AzDSAA. No information was provided how confidentiality of the measure can be achieved. | Except for the provision contained in Article 21/3, Azerbaijan is in line with the Convention. |

# 4 Belarus

## 4.1 Available documents and other sources

Belarus did not reply to the questionnaire. This part of the Report is based solely on the (1) country profile of Belarus, regarding its cybercrime legislation (from June 2011, provided by CoE Secretariat, hereinafter ByProfile), and (2) excerpts from various sources of the Belarus legislation, also provided by the CoE Secretariat. These sources include the Criminal Code, Code of Criminal Procedure (ByCPC), Law on Public Prosecution, Law on law enforcement authorities, Code on administrative offences, Law on operational investigative activity, Decree of the President of Belarus on the improvement of the national Internet segment, Decree of the President of Belarus approving the regulation governing interaction between telecom operators and investigation authorities and Law on international legal assistance in criminal matters.

## 4.2 Preliminary measures (articles 16 and 17 of the Convention)

In the aforementioned sources (4.1) there are several provisions which cover some of the issues which are the subject-matter of Articles 16 and 17. Some provisions, which in substance create a specific data retention system, are provided by the *Decree of the President of the Republic of Belarus on the improvement of the national Internet segment*. This decree mandates that:

(1) Internet service[32] providers[33] "identify user's terminals when providing services", and "register and store data on the users' terminals and information on Internet services provided".
(2) In addition, owners of Internet share points (computer clubs, Internet-cafes, home networks and other locations where public access to the Internet is possible) or persons authorised by them are required to enable identification of their Internet users and store their personal data and information on internet services provided to those users.

These types of information (1 and 2) should be stored for one year, and should be made available to various public authorities (investigation agencies, prosecutor's office, and initial investigation bodies, bodies of the State Control Committee, tax authorities, and courts) at their request and in accordance with the law.

The aforementioned provisions do not amount to an implementation of articles 16 and 17. While the system established in Belarus enables the retention of certain categories of computer data, which include also traffic data, it is not in line with the scope Articles 16 and 17, or their purpose.

## 4.3 Production order

According to ByProfile, article 18 of the Convention is implemented by provisions of the *Decree on Measures to Improve Use of the National Segment of Internet*, mentioned above (power of certain authorities to request data from ISP's, share point owners and other subjects). It is stated that those powers are regulated in more details in relevant acts.

In this context, the Law on Agencies of Internal Affairs is mentioned as an example. According to this law, internal affairs agencies are authorized to carry out operative investigations and to*, inter alia*, "request and receive from companies and people data and explanations as to inspected activity; to schedule inventory count and inspections; to request and, where necessary, seize documents, …".

[32] For the purposes of the decree, „Internet services shall be understood to mean services related to the provision of Internet access to legal entities and individuals, and/or posting, transmission, keeping, and modification of data in Internet".

[33] For the purposes of the decree, "Internet providers shall be understood to mean legal entities or sole proprietors rendering Internet services".

The only safeguard mentioned in this part of ByProfile is the obligation to compensate damage done during the execution of these measures.

On the basis of available information, it appears that it is possible to achieve the purpose of article 18 in part, where it relates to subscriber information. However, in this context, the issue of conditions and safeguards remains unsolved. On the other hand, it should be noted that the scope of article 18 is broader since it does not relate only to subscriber information but to any type of stored computer data. For these reasons, it cannot be concluded that Belarus implemented article 18 of the Convention in a valid manner.

## 4.4 Search and seizure of stored computer data

According to ByProfile, article 19 of the Convention is implemented in Belarus legislation via chapter 24 of the ByCPC. According to the article 208 of the ByCPC, search can be executed when there is reasonable evidence to believe that the instrument of crime, items, records, and valuables which may be critical for criminal investigation may be kept on specific location or held by specific person. In the similar manner, article 209 states that "reasonable evidence indicating that certain items or records which are critical for criminal investigation are available, provided that the location and possessor thereof have been clearly identified, constitutes grounds for a seizure".

From the formal viewpoint, it has to be emphasized that Belarus is the only of the project countries which does not provide for a judicial overview of the search and seizure measure. According to the article 210/1 of the ByCPC, "a search/seizure shall be supported by a warrant issued by an investigator/inquiry agency". However, in extraordinary circumstances, "a search can be conducted without a prosecutor's warrant" (ByCPC, 210/3), in which case a "search report shall be forwarded to the prosecutor within 24 hours".

To our best knowledge, articles 19/2-4 do not have corresponding provisions in ByCPC. Due to the fact that Belarus did not submit their reply to the questionnaire nor take part in the discussions, we were not able to analyse whether there are any other legal provisions which could be used to give effect to these measures.

In addition to the grounds justifying execution of search and seizure measures, ByCPC contains several other conditions and safeguards which regulate the application of these measures. These include, *inter alia*, special rules for "seizures conducted in private quarters or other legitimately occupied estate against the will of the owner or other occupants" (ByCPC, 210/2), requirement that attesting witnesses be present to the search (ByCPC, 210/4), requirement that the person against whom the search and seizure are directed be first given the opportunity to submit relevant objects voluntarily (ByCPC, 210/6,8), exclusion of certain places from the scope of search measures (diplomatic missions, consular agencies, and representative offices/missions of foreign countries and international organizations, ByCPC 210/10), etc. In addition, article 211 of the ByCPC mandates that search record be compiled and a copy of it be given to a person who has been subject to the search/seizure.

## 4.5 Real-time collection of traffic data

In relation to the real-time collection of traffic data, ByProfile stipulates that this measure is performed on the basis of the Law On Investigation Activities (ByLOIA). It seems that the relevant provision in this regard is article 11, sub-paragraph 12, which provides for a power to "retrieve information from telecom channels".

If interpreted correctly, and if real-time collection of traffic data is considered to be the measure which limits constitutional right to privacy, it would follow from article 13 of ByLOIA that this measure can only be executed on the basis of prosecutor's warrant, upon a "well-grounded order of a respective agency responsible for operational investigation". Article 13 also provides for certain time-limits of the duration of relevant measures.

## 4.6 Interception of content data

From the information available to us, it seems that the legal framework for the interception of content data is established in several sources of law. First, article 214 of the ByCPC provides for a general power to monitor and record communications. This article reads as follows:

> Article 214. Monitoring and Recording Communications
>
> 1. In investigating serious felonies, provided there is reasonable evidence to believe that telecom or other communications conducted by a suspect, offender or other individuals may contain data which are critical for the investigation, these communications may be monitored and recorded subject to the warrant issued by the prosecutor or deputy thereof, or, alternatively, subject to the resolution of the Republic of Belarus Interior Minister, Chairman of the National Security Committee, Vice-Chairman of the Government Audit and Supervision Committee – Head of Financial Investigations, or officials acting in their capacity.
>
> 2. The investigator/inquiry agency shall issue a well-grounded warrant specifying the need for monitoring/recording communications, indicating the particular criminal case and outlining reasons for such investigatory action. It shall also include first/middle/last name of the person(s) whose communications will be monitored/recorded, duration of monitoring, and the agency that will be technically responsible for monitoring/recording.
>
> 3. The investigator/inquiry agency shall forward the warrant to the respective institution for execution.
>
> 4. Monitoring/recording of communications may under no circumstances exceed the term of preliminary criminal investigation and shall be terminated by the resolution of the investigator/inquiry agency.
>
> 5. The investigator/inquiry officer may, throughout the entire duration of the investigatory measure, request recorded messages for examination and monitoring. Sealed messages are provided to the investigator/inquiry officer with a cover note specifying start/end time and appropriate technical parameters of the recording equipment.
>
> 6. The investigator/inquiry officer shall examine and monitor messages, seek inputs of SMEs (if appropriate), and draw up a summary report subject to the requirements set out in Articles 193 and 194 hereof. Such report shall contain a word-for-word representation of the part of the message relating to the criminal case. Recorded messages shall be attached to the report, and the part thereof which has no reference whatsoever to the case in question shall be eliminated after the completion of criminal proceedings.

From the technical perspective, the interception of content data is facilitated by Presidential Decree on Cooperation between Telecommunication Operators and Investigation Authorities.

## 4.7 Summary

Given that only limited information was made available, only a preliminary analysis has been possible at this stage.

| Article | Situation in Belarus legislation | Recommendation |
|---|---|---|
| 16 | Partially covered by the Decree of the President of Belarus on the improvement of the national Internet segment.<br>Not in line with Article 16. | Belarus might want to consider the implementation of a specific preservation order in the BeCPC. Subject-matter and the scope of such measure should be defined in accordance with Articles 16 and 17 of the Convention. |
| 17 | Partially covered by the Decree of the President of the Republic of Belarus on the improvement of the national Internet segment.<br>Not in line with Article 16. | Belarus might want to consider the implementation of a specific preservation order in the BeCPC. Subject-matter and the scope of such measure should be defined in accordance with Articles 16 and 17 of the Convention. |
| 18 | Only partially covered by the Decree mentioned above. | Belarus might want to consider the implementation of a specific production order in the BeCPC. Subject-matter and the scope of such measure should be defined in accordance with Article 18 and should cover computer data in general, traffic data and subscriber information. Application of such measure should be limited by appropriate conditions and safeguards, in accordance with Article 15. |
| 19 | No specific provisions on computer-related search and seizure; "traditional" rules on search and seizure are used.<br><br>Conditions and safeguards used are described above (4.4). | Belarus might wish to consider the implementation of specific provisions providing legal framework for computer-related search and seizure.<br>Articles 19/2-4 should be implemented, with appropriate conditions and safeguards.<br>Existing conditions and safeguards, mentioned above (4.4) should be kept in place. The fact that there is no judicial overview of search and seizure measure is obviously a specific problem of ByCPC. We consider this to be broader issue than only a question of implementation of Article 19. |
| 20 | Partially covered in the ByLOIA. More information needed. | Obviously, Belarus operates system of data retention and therefore it is possible to achieve the purpose of article 20 by using retained data. However, due to the limited information available and the absence of opportunity to discuss the application of measure in practice we are not able to make recommendations. More information is needed to adequately analyse Belarus legislation with regard to Articles 20 and 21. |
| 21 | Partially implemented. More information needed. | From the perspective of Article 15, absence of judicial or other independent supervision over the execution of the measure, evident from the provision of article 210/1 ByCPC which provides for a wide range of authorities competent to order interception of data, is particularly problematic.<br>However, due to the limited information available and the absence of opportunity to discuss the application of measure in practice we are not able to make recommendations. More information is needed to adequately analyse Belarus legislation with regard to Articles 20 and 21 |

# 5 Georgia

## 5.1 Available documents and other sources

This part of the Report (regarding Georgia) is based on (1) the Georgian reply to the Questionnaire sent to the countries of the Eastern Partnership (hereinafter: GE Reply), (2) Georgian Criminal Procedure Code (hereinafter: GeCPC), (3) Georgian Law on Operative Search Activity (hereinafter: GeLOSA), and (4) Roundtable discussion on Article 15 of the Budapest Convention (Strasbourg, France, 7 December 2012).

## 5.2 Expedited preservation of stored computer data

Georgia did not implement article 16 of the Convention as a standalone measure. It is submitted that the purpose of article 16 can be achieved using the procedure established in article 136, paragraph 1 of the GeCPC.

The translated text of article 136/1 GeCPC reads as follows:

> If there is a probable cause that the information or document important for the criminal case is kept in a computer system or data storage, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requesting relevant information or document.

In general, the subject-matter of article 136/1 of the GeCPC is the production order, which is an issue primarily relevant in the context of article 18 of the Convention. However, according to the GE Reply, the terms of this provision are of an open nature and can cover requests directed to any person (ISP, individual or an organisation). Taking into account the fact that any case of non-compliance could potentially be treated as tampering with evidence, which is a criminal offence under Georgian law, an order based on article 136/1 creates a significant legal obligation on the part of its addressee and can therefore be used to achieve the purpose of the Convention's article 16 (preservation in an expedited manner).

In order for article 136/1 to be applied, an elaborate set of conditions has to be fulfilled. As is explained in the Reply to the Questionnaire, an *"on-going formal investigation is an absolute prerequisite, although there is no differentiation as to the crimes. Also, the need for an investigative action in all cases shall be based upon the probable cause standard."* In addition, it follows from the text of art. 136/1 that a court order, issued on a motion of a prosecutor, is needed to apply this measure. The procedure for issuing such an order is regulated extensively in article 112 of the GeCPC.

In relation to the requirement of confidentiality, specified in paragraph 3 of article 16 Budapest Convention, it should be noted that the article 104 of the GeCPC contains a general provision which aims at ensuring the confidentiality of criminal proceedings. This provision is strengthened by article 374 of the Criminal Code which established criminal liability for disclosure of investigative data.

## 5.3 Expedited preservation and partial disclosure of traffic data

As regards the expedited preservation (and partial disclosure) of traffic data, no legal provision have been implemented in Georgian legislation to give effect specifically to this part of Articles 16 and 17. However, taking into account that traffic data are specific type of computer data in general, it is possible to use procedure described above to preserve traffic data as well. On the other hand, the preservation of traffic data is a specific task in the sense that it can require cooperation between several service providers when it is necessary to reconstruct the whole chain of communications.

According to the GE Reply, the mechanism of real-time collection of traffic data, provided in article 137 of the GeCPC, can be used in order to give effect to articles 16 and 17, when they relate to preservation of traffic data (held by multiple service providers). In addition to the legislative framework, some operational details regarding collection of traffic data in real time are regulated by the "Memorandum between the Law Enforcement Agencies and Internet Providers on the principles of cooperation in the field of cybercrime".

It was stated in the GE Reply that preservation of traffic data on the basis of article 137, while possible from the normative point of view, was yet not tested in practice. This issue was discussed further in the Strasbourg meeting, and it was underlined once again that the technical and legal framework for the execution of measure required in articles 16 and 17 of the Convention is in place, but has not yet been utilised.

As was explained *supra*, Georgian law enables preservation of computer data in general and traffic data in particular using production order and/or search and seizure measures. It is apparent from the legal framework which regulates these measures that their application presupposes that a detailed set of conditions and safeguards be satisfied. On the contrary, measures defined in Convention's articles 16 and 17 are the least invasive, compared to other provisions in Section 2. For these reasons, it is in theory possible to object to Georgian implementation of Articles 16 and 17 on the basis that those conditions and safeguards are making the whole procedure difficult to undertake, thereby depriving it of the possibility to be undertaken expediently. However, it was confirmed during the discussions for the preparation of this report that the Georgian authorities are in practice able to get the required orders and serve them in expedient manner, during the time-frame which they consider appropriate. For those reasons, it can be concluded that the purpose of Article 16 can be achieved in the current Georgian legislation.

## 5.4 Production order

Article 18 is implemented in Georgian law via article 136 of the GeCPC. The translated text of this article reads as follows:

> Criminal Procedure Code
>
> Article 136. Request for document or information
>
> 1. If there is a probable cause that the information or document important for the criminal case is kept in a computer system or data storage, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requesting relevant information or document.
>
> 2. If there is a probable cause that a person commits a crime though a computer system, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requesting a service provider to submit existed subscriber information.
>
> 3. For the purpose of this Article, 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 determined:
>
> a) the type of communication service used, the 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, which is 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.

4. Motions provided by paragraph 1 and 2 of this Article, shall be considered by the court in accordance with the procedure established by Article 112 of the present Code.

It is obvious from the wording and structure of the aforementioned provisions that they were drafted in accordance with the provisions of Convention's article 18. The first part of this article, which deals with the production order for computer data in general, is implemented in Georgian legislation via article 136/1 of the GeCPC. Provisions on the production order of subscriber information are implemented in paragraphs 2 and 3 of the same article.

The scope of these provisions, as well as their text and purpose are completely in line with the aforementioned provisions of article 18.

What are the conditions and safeguards which restrict the application of article 136?

While article 136 of the GeCPC can be used to investigate circumstances of any crime defined in the material part of criminal legislation, from the procedural point of view an on-going formal investigation is an absolute prerequisite for its application. Secondly, articles 136/1 (computer data in general) and 136/2 (subscriber information) can be used when there is probable cause that information important for criminal case will be found or that certain person (subscriber) committed a crime through computer system. For the purposes of GeCPC, probable cause standard is defined in article 13/11 of the GeCPC as

"a body of information or facts that in corroboration with all circumstances of a given criminal case would be sufficient for the reasonable person to conclude that a person has probably committed a crime; an evidential standard for conducting investigative activities directly prescribed by this Code and/or imposing preventive measure."

Since the measure defined in GeCPC 136 is considered to be an investigative action which intrudes into the private sphere of an individual, it can be carried out only on the basis of a court order. The procedure for issuing such an order, and the possibility of executing the measure without it in cases of urgency, is defined in detail in article 112 of the GeCPC, which reads as follows:

Article 112. Investigative Action Conducted on the Basis of a Court Order

1. An investigative action related to the restriction of one's private property, ownership or right to privacy of a dwelling, shall be carried out on the basis of a court order issued on the motion of the parties. A judge shall without the oral hearing decide on the motion within 24 hours from the moment of receiving a motion and other necessary information for reviewing the motion. A judge shall be authorized to consider the motion with participation of the party filing the motion. In this case rules for considering motions set forth in Article 206 of this Code shall apply. Consent of co-owner or one party to communication is sufficient to conduct investigative actions without the court order determined under this paragraph.

[…]

5. The investigative action referred to in Paragraph 1 of this article may be conducted without a court order, upon an investigator's ruling, in case of urgency, where delay may cause the destruction of factual data essential for the case or will make it impossible to obtain such data, or when an object, document, substance or any other object containing information is discovered during another investigative action (plain view concept), or when a real threat to a person's health or life exists. In this case a prosecutor shall notify a judge, having jurisdiction over the territory where

the investigative action has been carried out, or a judge having jurisdiction over the place of investigation, within 24 hours from the moment of starting an investigative activity and shall transfer a file or a criminal case (or copies thereof) that justify the necessity of taking urgent investigative actions. A judge shall make a decision on a motion without an oral hearing within 24 hours from receiving the materials. The judge shall be authorized to consider a motion with participation of the parties (if the criminal prosecution has begun), as well as with participation of the person, against whom the investigative action has been conducted. While considering a motion a judge shall probe the legitimacy of the investigative action carried out without a court decision. A judge shall be authorized to summon a person who conducted the investigative action without a court order for obtaining explanations from the person. In this case rules for considering motions set forth in Article 206 of this Code shall apply.

6. After examining the case materials a court shall render an order on:

a) finding the investigative action legitimate;

b) finding the investigative action illegitimate and the collected information to be inadmissible evidence.

7. The judge has the right to consider the matters under this Article without an oral hearing.

8. The order issued pursuant to this article may be appealed in accordance with the rules set forth in the article 207 of this Code. The term for appeal shall be calculated from the enforcement of an order.

As regards the application of article 136, it was stated in the GE Reply and confirmed during discussions that the aforementioned provisions are routinely and successfully applied in practice. In addition, it was underlined that more informal cooperation between law enforcement agencies and ISPs is based on the "Memorandum between the Law Enforcement Agencies and Internet Providers based on the principles of cooperation in the field of cybercrime", which was concluded in 2010 and is still operational today. Article 4 of the Memorandum specifically obliges the ISPs to make available, in a confidential manner, information requested by law enforcement agencies. In practice, responses to LEA requests are provided within 3 days at average.

## 5.5 Search and seizure of stored computer data

Georgian legislation did not implement Article 19 of the Convention as a specific measure applicable for computer-related search and seizure; instead, traditional measures of search and seizure are applicable also to computer system and data.

General rules establishing grounds for search and seizure are contained in article 119 of the GeCPC, which reads as follows:

**Article 119. The Purpose and Grounds for Search and Seizure**

1. If there is a probable cause, a search and seizure shall aim at uncovering and seizure of any object, document, substance, or other item that contains information related to the case.

…

3. An object, document, or other item including information relevant to the case may be seized if a there is a probable cause that the object, document, or other item is kept in a certain place, with a certain person, and if it is not necessary to search for it.

4. It shall be possible to conduct a search for a seizure of an object, document, or other item including information relevant to a certain case, if there is a probable cause, that it is kept in a certain place, with a certain person, and if search is necessary for discovering it.

An on-going formal investigation is an absolute prerequisite for the execution of search and seizure measures. According to the GeCPC, search and seizure are executed on the basis of a court order.

As regards article 19/2 of the Convention, there are no provisions in Georgian legislation which would specifically enable extension of a search to another system so a new order would be necessary to do so. It is submitted, however, that in exigent circumstances a new order can be obtained urgently. In that case only a prosecutor's ruling would be necessary, and judicial review and approval would be obtained subsequently.

Since there are no specific rules for cases of computer-related search and seizure, Article 19/3 of the Convention is also not given effect via particular rules in GeCPC. However, it was explained during the discussions that bodies that perform seizure measures in practice have the possibility to apply the powers defined in Article 19/3.

Article 19/4 is not implemented. However, it was submitted that in theory it is possible to order a person to provide necessary information under the witness status. According to article 3(20) of GeCPC, a witness is a person who might be aware of the facts necessary for ascertaining the circumstance of the criminal case. Hence, this provision can be also applied to a person who possesses the necessary knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide. Since the denial of testimony or bearing false testimony by the witness is a criminal offence under the Georgian Criminal Code (articles 370 and 371), it is argued that the purpose of Article 19/4 can be achieved in the indirect manner.

The procedure for execution of search or/and seizure measures is regulated in detail in article 120 of the GeCPC, which reads as follows:

**Article 120. The Rule for Search and Seizure**

1. On the basis of a court order or in case of urgency – on the basis of ruling – authorizing search or seizure, an investigator shall have the right to enter storage, dwelling, or other ownership for the discovery and seizure of an object, document, or other item containing relevant information for the case.

2. Prior to a search or a seizure the investigator shall be obliged to present a court order or in case of urgency – a ruling, to a person subject to search and seizure. The presentation of the order (ruling) shall be confirmed by the signature of the person.

3. While the search/seizure is being conducted, an investigator shall have the right to restrict the person(s) at the place of search/seizure from leaving and from communicating with one another or with other persons. This shall be reflected in the relevant record.

4. Upon presenting a court order, in case of urgency – ruling, the investigator shall offer the person subject to search or seizure to voluntarily turn over the object, document, or other item containing relevant information. If the item to be seized is voluntarily turned over, it shall be noted in the record; in case of refusal to turn over the requested item voluntarily or in case of its partial disclosure the seizure by coercion shall take place.

5. During the search the object, document, substance, or other item containing information, which is indicated in the court order or ruling shall be searched for and

seized. Any other object containing information that might have an evidentiary value on the concerned case or that might clearly indicate on other crime, as well as the object, document, substance and/or other item removed from the circulation may also be seized.

6. Items containing information, objects, documents, substances, or other relevant items discovered during the search or seizure shall be presented to the persons participating in the investigative action if possible prior to the seizure. Upon the presentation, they shall be seized, described in detail, sealed, and packaged, if possible. Apart from the seal, the packaged items shall reflect the date and signatures of the persons participating in the investigative action.

7. During the search and seizure the investigator shall have the right to open a closed storage or premise if the person to be searched refuses to do so voluntarily.

8. If there is a probable cause that the person present at the place of search or seizure has hidden the object, document, substance, or other item to be seized, personal search of such person shall be allowed. Such case shall be regarded as urgent necessity and, shall be conducted without a court order or a investigator's ruling. The legitimacy of search and/or seizure shall be reviewed by the court in accordance with the rules established by this Code.

9. Search or seizure in the building of a legal entity or an administrative body shall take place in the presence of the head or a representative of that entity or the body.

In addition, additional conditions and safeguards are provided for cases when it is necessary to execute a search at diplomatic premises and offices of mass–media, publishing houses, scientific, educational, religious and public organizations and political parties. These issues are regulated in GeCPC, article 122[34] and 123[35].

## 5.6 Real-time collection of traffic data

[34] Article 122. Search and Seizure at the Premises of a Diplomatic Mission and of a Diplomat

1. Search or seizure on the territory of a Diplomatic Mission or of a person enjoying diplomatic immunity as well as inside a building or a transport facility occupied by a diplomat or a member of his/her family shall only be permitted with a consent or upon request of the head of the Diplomatic Mission.

2. The permission of the Head of Diplomatic Mission to conduct search or seizure shall be sought through the Ministry of Foreign Affairs of Georgia.

3. In the case(s) referred to in Paragraph 1 of this article, it shall be obligatory to have a representative of the Ministry of Foreign Affairs of Georgia attend search or seizure.

[35] Article 123. Procedure for Search, Seizure and Arrest of Property at the Offices of Mass–Media, or at the Premises of Publishing Houses, Scientific, Educational, Religious, Public Organizations and Political Parties

1. Objects, documents, articles or other items containing scientific or educational information may not be searched, seized or arrested from the offices of mass-media, or from the premises of publishing houses, scientific, educational religious, public organizations or political parties, toward which reasonable expectation of public release exists;

2. The restriction referred to in Paragraph 1 of this Article shall not apply if there is a probable cause that the object, document, substance or other item containing information to be seized represents the subject or tool of a crime.

3. A court is authorized to adopt ruling regarding the search, seizure and/or arrest only in a case, when there is obvious and reasonable ground that the conduct of an investigative action would not violate right to freedom of speech, opinion, conscience belief, religion, or right to union guaranteed under the Georgian constitution. The investigative action shall be conducted in an effective form to provide for most minimal restriction of these rights.

Article 20 of the Convention is implemented in Georgian legislation via article 137 of the GeCPC, which reads as follows:

> **Article 137. Real-time collection of traffic data**
>
> 1. If there is a probable cause that a person commits a crime though a computer system, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requesting real-time collection of traffic data, thereby a service provider is obliged to cooperate with and assist an investigative body in real-time collection or recording of traffic data which are associated with specified communications made and transmitted by means of a computer system within the territory of Georgia.
>
> 2. Motions provided by paragraph 1 of the present Article shall consider technical capability for real-time collection and recording of traffic data of the service provider. The term for real time collection and recording of traffic data shall not exceed the term necessary for collecting evidence in criminal case.
>
> 3. Motions provided by paragraph 1 and 2 of this Article, shall be considered by the court in accordance with the procedure established by Article 112 of the present Code.

Conditions and safeguard used in connection with this measure generally follow the same principles as in cases of other procedural measures required by the Convention (production order and search and seizure). While the on-going formal investigation is an absolute prerequisite for this measure also, Georgian law makes no differentiation as to the crimes for which it can be applied.

Regarding other conditions, this investigative method is also conducted on the basis of a court order. In that respect, article 112 GeCPC, cited above, is applicable. Also, the need for an investigative action in every particular case assessed upon the probable cause standard (GeCPC, 137/2).

## 5.7 Interception of content data

Article 21 of the Convention is implemented in Georgian legislation via article 138 of the GeCPC, which reads as follows:

> **Article 138. Interception of content data**
>
> 1. If there is a probable cause that a person commits a crime through computer system, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requiring interception of content data, thereby a service provider is obliged to cooperate with and assist an investigative body in real-time collection or recording of content data which are associated with communications made and transmitted by means of computer system within the territory of Georgia.
>
> 2. Motions provided by paragraph 1 of the present Article shall consider technical capability for real-time collection and recording of traffic data of the service provider. The term for real time collection and recording of traffic data shall not exceed the term necessary for collecting evidence in criminal case.
>
> 3. Motions provided by paragraph 1 and 2 of this Article, shall be considered by the court in accordance with the procedure established by Article 112 of the present Code.

Conditions and safeguards include the need for an on-going formal investigation, probable cause, court order, limitation in time. However, Georgian legislation notably lacks any limitation in the

application of the interception measures with regard to the differentiation of the crimes. This is not in line with Article 21/1, which stipulates that measures defined therein should be used "in relation to a range of serious offences to be determined by domestic law". In its present form, the solution used in GeCPC may be criticized as lacking the proportionality required by Article 15.

It was stated in the GE Reply that the overall procedure for interception of traffic data does not involve any additional steps or checks besides those in Art. 138.

In addition, it was submitted that it is possible that actions referred to in Art. 138 are in practice applied also according to the provisions of the GeLOSA:

> **Article 7. Definition of Operative-Investigative Activity**
>
> 1. Operative-Investigative Activity is an activity of the authorized public agency or an official determined by the Law, who ensures performance of the goals provided by Article 2 of the present Law within its competence.
>
> 2. For the performance of these goals an authorized public agencies openly or through preserving conspiracy rules use following measures:
>
> […]
>
> h) Hidden recording of or eavesdropping on telephone conversation, receiving information and fixing from transmission lines (though connection to transmission means, computer networks, streamline communication) from computer system (directly or remotely) and for this purpose installation of relevant software devices; control of postal and telegraphic parcels (except diplomatic post) based on the order of the court.
>
> The evidence obtained in this manner can be used in criminal cases as admissible evidence, although no practice this effect has been reported in cybercrime cases throughout 2011-2012.

Not enough information was provided about the scope of GeLOSA in relation to the execution of the interception measure. It appears, however, that most of the conditions and safeguards present in the GeCPC are applicable in the case of GeLOSA.

## 5.8 Summary

| Article | Situation in the Georgian legislation | Recommendation |
|---|---|---|
| 16 | Article 16 is given effect by the production order, in a manner consistent with the requirements of the Convention. | Georgia is in line with Article 16. However, with the aim of achieving the full purpose of the Section 2, Georgia might want to consider the implementation of specific preservation order, since the availability of such measure would increase the flexibility of Georgian criminal justice system. |
| 17 | Article 17 is implemented by a combination of production order and agreements on cooperation between Georgian authorities and communication service providers. | Georgia is in line with Article 17. However, with the aim of achieving the full purpose of the Section 2, Georgia might want to consider the implementation of specific preservation order, since the availability of such measure would increase the flexibility of Georgian criminal justice system. |
| 18 | Implemented in line with the Convention. | Georgia is in line with Article 17; the only reservation being article 136/2, which can be applied only to |

| | | |
|---|---|---|
| | | "crimes committed through a computer system". In line with Article 14, this should be broadened to enable collection of evidence in electronic form of any crime. |
| 19 | No specific provisions on computer-related search and seizure; "traditional" rules on search and seizure are used.<br><br>Conditions and safeguards used are described above (5.5). | Georgia might wish to consider the implementation of specific provisions providing legal framework for computer-related search and seizure.<br><br>Different options of seizing and similarly securing computer data, enumerated in Article 19/3, should be explicitly enumerated in transposed in GeCPC and Article 19/4 should be implemented, all with the appropriate conditions and safeguards.<br><br>Existing conditions and safeguards, mentioned above (5.5) should be kept in place. |
| 20 | Implemented in line with the Convention. | Georgia is in line with Article 20. |
| 21 | Partially implemented. | Georgia might wish to limit the application of GeCPC 138 to a range of serious offences. |

# 6 Republic of Moldova

## 6.1 Available documents and other sources

This part of the Report (regarding the Republic of Moldova) is based on the following sources: (1) Moldovan reply to the Questionnaire sent to the countries of the Eastern Partnership (hereinafter: MD Reply); (2) Moldovan Law on Preventing and Combating Cybercrime (hereinafter: MdLPCC); (3) Moldovan Criminal Procedure Code (hereinafter: MdCPC) and (4) Moldovan Law on Special Investigative Activity (hereinafter: MdLSIA).

## 6.2 Expedited preservation of stored computer data and traffic data, and partial disclosure of traffic data

According to the MD Reply, measures defined in articles 16, 17 and (in part) 18 of the Convention are implemented in the Moldovan legal system via article 7 of the MdLPCC.

The translated text of this article reads as follows:

> **Article 7.** Obligations of service providers
>
> (1) Service providers are obliged:
>
> a) to keep records of service users;
>
> b) to notify the competent authorities about the web traffic data, including the data about illegal access to computer system information, about the attempts to introduce illegal programs, about the violation by competent persons of the rules of collection, processing, storage, transmission and distribution of information or of rules of computer system protection provided according to the information importance or to its degree of protection, if they have contributed to acquisition, distortion or destruction of information or if they have caused other serious consequences, perturbation of computer systems functioning and other computer crimes;
>
> c) to perform, confidentially, the competent authority's request regarding the immediate preservation of computer data or of web traffic data, which are in danger of destruction or alteration, within 120 calendar days, under the provisions of national legislation;
>
> d) to submit to the competent authorities, on the basis of a request made under the law, the data about users, including the type of communication and the service the user benefited by, the method of payment for the service, as well as about any data that can lead to the identification of the user;
>
> e) to undertake security measures by means of using some procedures, devices or specialized computer programs, with the help of which to restrict or forbid the unauthorized users to access a computer system;
>
> f) to ensure the monitoring, supervision and storage of web traffic data for a period of at least 180 calendar days, in order to identify service providers, service users and the channel by means of which the communication has been transmitted
>
> g) to ensure the interpretation of computer data from network protocols packages, preserving such data for a period of at least 90 calendar days.
>
> (2) If the web traffic data are possessed by several service providers, then the requested service provider is obliged to submit to the competent authority the necessary information for the identification of the other service providers.

In relation to the aforementioned provisions, it is also necessary to take into account article 2 of the same law, which contains definitions of the terms used in article 7. Article 2 reads as follows:

> **Article 2.** Definitions
>
> In the present law, the following main concepts mean:
>
> *Computer system* – any remote device or a set of interconnected or connected devices, which ensure (or one or more of its components ensure) the automatic data processing by implementing a program;
>
> *Computer data* – any facts, information or concepts in a form suitable for processing in a computer system, including a program able to determine the performance of a function by a computer system;
>
> *Service provider* – any public or private entity which offers to its users the possibility to communicate through a computer system, as well as any other entity that processes or stores computer data for this communication system or for its users;
>
> *Web traffic data* – any data related to a communication transmitted through a computer system, generated by this system as a part of the communication chain, indicating the origin, destination, route, hour, date, size, duration or type of underlying service;
>
> …

## 6.3 Expedited preservation of stored computer data in general

Article 7 paragraph c of the aforementioned MdLPCC creates an obligation for service providers to, at the competent authority's request, immediately preserve computer data in general, as well as traffic data, which are in danger of destruction or alteration. While this article covers the whole subject-matter of Articles 16 and 17 in relation to relevant types of data, it is significantly limited in scope since its obligation to preserve data can only be used against service providers.

During the discussions for the preparation of this Report, it was explained that public prosecutors have the authority to issue preservation orders on the basis of article 7/c MdLPCC. These orders do not require judicial confirmation; however, in order to obtain preserved data it is necessary to use a production order which is issued by the court.

Regarding the scope of Article 16, it would be possible to claim that data held by persons other than service providers can be "preserved" using search and seizure measure. However, based on the information provided during the discussions it is questionable that such a procedure could be conducted in an expedited manner. For these reasons, the Republic of Moldova might wish to broaden the scope of article 7 MdLPCC so that it covers all the subjects, and not only service providers, who might be in control of specific computer data.

## 6.4 Expedited preservation and partial disclosure of traffic data

Provisions found in article 7 paragraph c of the MdLPCC are, as they relate to "web traffic data", strengthened by paragraph f of the same article, according to which service providers are required to *"ensure the monitoring, supervision and storage of web traffic data for a period of at least 180 calendar days, in order to identify service providers, service users and the channel by means of which the communication has been transmitted"*.

In the context of preservation of traffic data, article 7 MdLPCC is an adequate tool to achieve the purpose of Article 16. First, it has to be noted that the definition of the term "web traffic data", which is subject matter of article 7/c, is identical to the one given in the Convention. Also, article

7/c gives effect to paragraph 3 of Convention's article 16 (requirement of confidentiality). In addition to the requirements under article 16, article 17 requires that Parties also enable expedited preservation of traffic data in cases where more than one service provider is involved in the chain of communication. This provision is implemented in Moldovan legislation by the second paragraph of article 7 MdLPCC.

One specific difference between the Convention and MdLPCC concerns the duration of the order to preserve data: article 7/c provides for a period of 120 days, while the Convention stipulates that 90 days period should be used, but with the possibility to renew the order.

Regarding the Article 17, and with the reservation concerning 90-120 days preservation time, the Moldovan legislation is completely in line with the Convention.

## 6.5 Production order

Article 18 is not fully implemented in the Moldovan legislation. In relation to obtaining access to stored computer data in general, Moldovan authorities can only use standard seizure measures. As regards subscriber information, article 7 of the MdLPCC prescribes that communication service providers are obliged:

> a) to keep records of service users;
>
> …
>
> d) to submit to the competent authorities, on the basis of a request made under the law, the data about users, including the type of communication and the service the user benefited by, the method of payment for the service, as well as about any data that can lead to the identification of the user;

However, the scope of information collected on the basis of these provisions remains unclear.

## 6.6 Search and seizure of stored computer data

In Moldovan legislation, there are no provisions which would provide a legal framework specifically for the search and seizure of computer data. Instead, general rules of traditional search and seizure measure are used to give effect to the Convention's article 19.

Rules on search and seizure are found in MdCPC, articles 125 – 132. At the beginning, it should be noted that an open criminal investigation is a general requirement for the execution of this measure.

The terms "computer system" and "computer data" are not defined nor are they used in MdCPC. However, it was confirmed during the discussions held for the purpose of preparation of this report that their subject matter is covered, for the purposes of MdCPC, by the terms "objects" and "documents", and that measures defined in the Convention's article 19/1 are in practice executed on the basis of these provisions.

As a general rule, a search can be conducted when, based on existing evidence, if there are sufficient grounds (one can "justly presuppose") that objects and documents which are of interest for the criminal case can be found in a certain place or with a certain person (125/1).

From the formal point of view, the standard legal ground for executing a search is an order issued by the judge of the investigation ("instruction judge")[36], upon a motion of a criminal prosecution body (125/3). In limited circumstances, it is possible that a search be done upon a reasoned order issued by the body of criminal prosecution (125/4). Such an order has to contain a statement of reasons and be submitted to the judge as soon as possible, but not later than 24 hours since the measure was conducted (125/4). The judge in charge of investigation will subsequently verify the legality of the procedural action and declare it valid or invalid (125/5).

In relation to article 19/2, it has to be noted that MdCPC does not contain specific provisions aimed at implementation of the measure defined therein. It was stated during the discussion that in practice a new search warrant would be required for each connected system that is searched.

According to article 19/3, Parties to the Convention should also enable its competent authorities to seize or similarly secure computer data found during conducting a search. In this respect, provisions of articles 126 and 128 of the MdCPC apply.

According to article 126/3, the seizing of objects and documents can be done on the basis of an explained and motivated warrant issued by the criminal prosecution body. For these rules to apply, it is necessary that accumulated evidence or information from an ongoing investigation show location or persons who are in possession of objects which are being seized, and that those objects are important for the particular criminal case (126/1). As an exception, seizure of those items that contain information which constitute state, trade or banking secrets and telephone conversations requires judicial authorisation (126/2).

The procedure for seizing objects and documents is regulated in more detail in article 128. According to its paragraph four, after submitting the warrant, the representative of the criminal prosecution body will request the handing over of objects or documents that need to be sequestrated. Should this request be refused, the criminal prosecution agent then proceeds to forced seizing. If the items that need to be sequestrated are absent from the place indicated in the warrant, the criminal prosecution agent has the right to perform the search, justifying the necessity of carrying out this action. In that case, however, authorisation of a judge is necessary in order to enter a domicile or other private premises (128/2).

Article 19/3 of the Convention specifies that a seizure measure should include the powers to (i) seize or similarly secure a computer system or part of it or a computer-data storage medium; (ii) make and retain a copy of those computer data; (iii) maintain the integrity of the relevant stored computer data and (iv) render inaccessible or remove this computer data in the accessed computer system.

These provisions have no counterparts in the MdCPC. However, as stated in MD Reply and confirmed in discussions, in practice criminal investigation bodies can, at their discretion decide to make and retain copies of computer data or seize the whole computer system or its part.

The power defined in article 19/4 is not defined in MdCPC.

In addition to the conditions described *supra*, additional safeguards connected with the application of search and seizure measures, defined in MdCPC, are the following:

- Presence of certain persons is required during search (person against whom the measure is applied, or members of her family, or other person who represents her

[36] See article 6/24 of the MdCPC, where the term instruction judge is defined as "a judge given prerogatives belonging to the prosecution and of judiciary control on procedural actions made during the criminal investigation".

interests; representative of enterprises or organizations whose premises are being searched)37

- It is forbidden to conduct a search during night time (128/1)
- A search warrant has to be given to the person whose premises are being searched (128/3)
- The criminal prosecution body is obliged to take measures to ensure that circumstances connected to the private life of the person, noticed during the search or seizing, are not disclosed to the public (128/9).

## 6.7 Real-time collection of traffic data

Article 20 of the Convention is not implemented in the Moldovan legislation. In addition, it was confirmed that currently criminal prosecution authorities in Moldova do not collect traffic-data in real time, since they do not possess adequate technical capabilities to implement this measure.

## 6.8 Interception of content data

The general legal framework for the interception of communications (its content data) is established in articles 135 and 136 of the MdCPC. According to article 135/1, these provisions cover telephone and radio communications and communications achieved using other technical means. However, it was stated in MD Reply and confirmed in discussions that Moldovan criminal prosecution bodies currently do not have technical capabilities to realize the measure of interception communications transmitted via Internet. While, for that reason, we can conclude that article 21 is not given full effect in Moldova, we will nevertheless analyze legal framework for interception of communications, which will naturally become applicable once the technical means are established.

As a general principle, an open criminal investigation/criminal proceeding is the basic requirement for the execution of this measure. In addition, article 135 (interception of communication) can only be applied in relation to the limited catalogue of criminal offences – so called extremely serious and exceptionally serious crimes.

The measure of interception of communications can only be ordered by the investigating judge upon a reasoned motion of the prosecutor (135/1). However, in case of urgency, when there is danger that the delay in execution of measure could harm the evidence collection procedure, the prosecutor is allowed to issue a motivated ordinance allowing interception and recording of communications on her own, and inform the judge of the investigation about it immediately, and in any case no later than 24 hours (135/2). Following that, a judge is required to confirm the order of the prosecutor and authorize the measure in the next 24 hours, or order its suspension and destruction of already made records (135/2).

The interception of communication can only be ordered for a maximum of 30 days. If justified, it can be prolonged, but every time only for additional 30 days. The total duration of the measure may not exceed 6 months or last longer than the criminal prosecution (135/4). Also, if the grounds (reasons) on which it was ordered cease to exist, the execution of the measure must stop immediately.

Some additional conditions and safeguards are provided in article 136 of the MdCPC, which translated reads as follows:

[37] MdCPC, article 127.

Article 136. Interception and recording and their authorization

(1) Interception of communications are carried out by the criminal prosecution body. Persons whose responsibility is to technically facilitate interception and recording of communications are obliged to preserve the secret of the procedural action and confidentiality of correspondence. They are liable in case of violation of their obligation according to provisions of articles 178 and 315 of the Criminal Code. An entry regarding explaining these obligations is made in the minute of the interception.

(2) A minute regarding interceptions and recording performed by the criminal prosecution body is drawn up in conformity to provisions of articles 260 and 261. The authority given by the instruction judge is additionally mentioned here along with the indication of telephone number, or numbers, the addresses of the telephone posts, radio or other technical means used to carry out the conversations. The record will also indicate the name of persons, whenever they are known, date and time of each separate conversation and number assigned to the tape used for recording.

(3) Recorded communications are integrally transcribed and annexed to the minutes along with the authorization from the criminal prosecution body, after its verification and signing by the prosecutor carrying out or supervising the criminal prosecution. Correspondence in other languages than the one in which the criminal prosecution is carried out is translated with the assistance of an interpreter. The tape containing the original recorded communication is also annexed to the minutes after having been sealed and the stamp of criminal investigation body has been applied.

(4) The tape with the recorded communication, its written version on paper and the minutes of the interception and recording of communications are handed over to the prosecutor within 24 hours period of time. The prosecutor assesses which one of the collected information is important for the respective case and draws a minutes in this respect.

(5) Original copies of the tapes along with the integral written version on paper and copies of minutes are handed over to the instruction judge who authorized interception of the communication for further storage in special place, in the sealed envelope.

(6) The court makes a decision or passes a sentence regarding destruction of records which are not important for the criminal case. All the other records will be kept up to the moment when the file is submitted to the archive.

## 6.9 Summary

| Article | Situation in the Moldovan legislation | Recommendation |
|---|---|---|
| 16 | Partially implemented, covers only preservation by service providers | The Republic of Moldova might wish to consider the implementation of a specific preservation order in the BeCPC, or broaden the scope of MdLPCC to give effect to Article 16 also in relation to other holders of data (beside service providers). |
| 17 | Republic of Moldova is in line with Article 17. | |
| 18 | Article 18 is only partially implemented (in relation to subscriber information). | Republic of Moldova might wish review its legislation in the light of Article 18 and introduce appropriate provisions enabling production order for computer data in general. As regards subscriber information, it is necessary to examine the scope of information communication service providers (according to article 7 of the MdLPCC) are preserving and verify that it |

| | | |
|---|---|---|
| | | includes all the data that the Convention defines as "subscriber information". |
| 19 | No specific provisions on computer-related search and seizure; "traditional" rules on search and seizure are used.<br><br>Conditions and safeguards used are described above (6.4). | Republic of Moldova might wish to consider the implementation of specific provisions providing legal framework for computer-related search and seizure.<br>Situation envisioned in Article 19/2 should be addressed in specific provisions in MdCPC. Different options of seizing and similarly securing computer data, enumerated in Article 19/3, should be transposed in MdCPC.<br><br>Article 19/4 should be implemented, with appropriate conditions and safeguards.<br><br>Existing conditions and safeguards, mentioned above (6.4) should be kept in place. |
| 20 | Not implemented. | Republic of Moldova might wish to consider the implementation of specific provisions providing legal framework for real-time collection of traffic data. |
| 21 | Republic of Moldova is in line with Article 21. | |

# 7 Ukraine

## 7.1 Available documents and other sources

Ukraine did not reply to the questionnaire sent to the countries of the Eastern Partnership. Therefore, this part of the report is based solely on the (1) Textual analysis of the new Ukrainian Criminal Procedure Code, which entered into force on 19 November 2012 (hereinafter: UaCPC), and (2) information provided during the Roundtable discussion on Article 15 of the Budapest Convention (Strasbourg, France, 7 December 2012).

## 7.2 Expedited preservation of stored computer data

Ukrainian CPC does not contain any specific provisions which would aim at implementation of Article 16. However, a number of other provisions may be used with the effect of securing stored computer data by other means than by preservation order. In this context, procedure of "temporary access to objects or documents", covered by articles 159 – 166 of the UaCPC, might be relevant. These provisions are discussed further in the text (7.4). However, with regard to all of these options, it should be taken into account that the new UaCPC was enacted only recently. For this reason, it was not possible to collect relevant information which would give sufficient insight into its application in practice.

From the perspective of Article 16, it should be noted that "temporary access to objects or documents" is allowed on the basis of a court decision. Such a decision is issued upon a motion to allow provisional access to objects and documents. According to UaCPC 163/1, upon a motion to order temporary access, an investigating judge or the court shall summon the person who possesses objects and documents needed. According to UaCPC 163/3,

> 3. In the ruling to summon the person who possesses such objects and documents, investigating judge shall state that objects and documents should be preserved in the condition in which they are at the moment of receiving court summons.

However, according to UaCPC 163/2,

> 2. If the party to criminal proceedings that filed the motion proves the presence of sufficient grounds to believe that a real threat exists of altering or destruction of the objects and documents concerned, the motion may be considered by investigating judge, court without summonsing the person who possesses them.

While the abovementioned provisions do not implement preservation orders in a manner which is compatible with Article 16, they could in theory be used to achieve purposes which are similar to those envisioned in the Convention.

However, with regard to these options, it should be taken into account that the new UaCPC was enacted only recently. For this reason, it was not possible to collect relevant information which would give sufficient insight into its application in practice.

## 7.3 Expedited preservation and partial disclosure of traffic data

According to the Ukrainian Law on Telecommunications (article 39), operators and providers of telecommunication services are required to retain some data on telecommunication services for a period of three years. Production of those data is theoretically possible on the basis of a production order ("temporary access to objects or documents", articles 159 – 166 of the UaCPC). Since there are no specific provisions regulating partial disclosure in the case of communication via multiple providers, the only usable option would be to serve warrants for temporary access to objects and documents to all of the providers concerned.

## 7.4 Production order

Ukrainian legislation does not implement Article 18 directly. However, the purpose of this article can partially be achieved by so-called "provisional access to objects and documents", which is regulated in chapter 15, articles 159-166 or the UaCPC. The purpose of chapter 15 of the UaCPC is to enable party to the criminal proceeding with the opportunity to examine objects and documents, make copies of them and seize them (UaCPC, 159/1). According to article 99 UaCPC, the term document is defined as follows:

> 1. A document shall mean a material object, which was created specifically for conservation of information, such object containing fixed by means of written signs, sound, image etc. the knowledge that can be used as evidence of the fact or circumstance which is established during criminal proceedings.
>
> 2. Documents, on condition of containing the knowledge specified in the first paragraph of this Article, may be:
>
> 1) materials of photography, sound recording, video recording and other data media (including electronic);

Provisional access to objects and documents is executed on the basis of a decision made by the investigating judge or the court (UaCPC 159/2), and issued upon a motion approved by a public prosecutor (UaCPC 160/1). Article 160/2 of the UaCPC stipulates the details of a motion which should be submitted for approval by the investigating judge / court. Details of the court's decision on provisional access are regulated by article 164.

The procedure for issuing of order on provisional access is regulated by article 163 of the UaCPC, which reads as follows:

> **Article 163. Consideration of the motion for provisional access to objects and documents**
>
> 1. After having received motion for provisional access to objects and documents, investigating judge, court shall summon the person who possesses such objects and documents, with the exception of the case specified in part two of this Article.
>
> 2. If the party to criminal proceedings that filed the motion proves the presence of sufficient grounds to believe that a real threat exists of altering or destruction of the objects and documents concerned, the motion may be considered by investigating judge, court without summonsing the person who possesses them.
>
> 3. In the ruling to summon the person who possesses such objects and documents, investigating judge shall state that objects and documents should be preserved in the condition in which they are at the moment of receiving court summons.
>
> 4. Investigating judge, court shall consider the motion with participation of the party to criminal proceedings which filed the motion, and the person who possesses the objects and documents, except as provide otherwise by the second paragraph of this article. Non-compliance with court summons of a person who possesses the objects and documents, without valid reasons, or his failure to inform of the reasons for non-appearance, shall not be obstacle for considering the motion.
>
> 5. Investigating judge, court shall issue the ruling to grant provisional access to objects and documents if the party to criminal proceedings proves in its motion the existence of sufficient grounds to believe that the objects or documents:

1) are or can be in possession of a physical or legal person;

2) per se or in combination with other objects and documents of the criminal proceedings concerned, are significant for establishing important circumstances in the criminal proceedings;

3) are not or do not include such objects and documents as contain secrets protected by law.

6. Investigating judge, court issue the ruling to grant **provisional** access to objects and documents containing secrets protected by law, if a party to criminal proceedings, in addition to circumstances specified in part five of this Article, proves the possibility to use as evidence the information contained in such objects and documents, and impossibility by other means to prove the circumstances which are intended to be proved with the help of such objects and documents.

The access of a person to objects and documents containing secrets protected by law shall be granted according to the procedure laid down by law. Access to objects and documents containing information that is a State secret, may not be granted to a person who has no security clearance as required by law.

7. Investigating judge, court in a ruling on the **provisional** access to objects and documents may order that possibility be provided for seizure of objects and documents, if a party to criminal proceedings proves the existence of sufficient grounds to believe that without such seizure, a real threat exists of altering or destruction of the objects and documents, or that such seizure is necessary for attaining the goal of obtaining the access to the objects and documents.

Certain categories of information are excluded from the scope of this order (article 161), or are subject to additional conditions and safeguards (article 162). In the latter category, UaCPC mentions also "information held by telecommunication operators and providers on communications, subscriber, rendering of telecommunication services including on receipt of services, their duration, content, routes of transmission etc.;" (article 162/7).

Although the rules in chapter 15 of the UaCPC are able to produce results similar to those required in Article 18, there are nevertheless several important differences.

In general, rules in UaCPC's chapter 15 are rules on seizure, not on production of data. This follows clearly from the text of UaCPC 165/1, which states that the person named in a decision on provisional access … "shall be required to give provisional access to objects and documents specified in the ruling to the person indicated in the investigating judge's, court's ruling". In this context, it should be noted that "access to document" is not the same as the "production of document".

On the other hand, article 165/1 contains an important safeguard, according to which

4. Upon demand of possessor, the person who produces the ruling on provisional access to objects and documents, shall be required to leave copies of seized documents. Copies of seized documents shall be made using copying equipment, electronic means of the possessor (upon his consent) or copying equipment, electronic means of the person who produces the ruling on provisional access to objects and documents.

From the perspective of Article 18, it should also be noted that article 162/7 of the UaCPC recognizes the fact that access to information possessed by providers of communication services (which covers at least some of the information defined as "subscriber information" in Article 18)

may be subject to additional limitations. However, we were unable to establish what those limitations might be.

## 7.5 Search and seizure of computer data

Ukrainian legislation does not provide for specific provisions regulating computer-related search and/or seizure; instead, traditional measures of search and seizure are applicable also to computer system and data.

General rules establishing grounds for search measure are contained in article 234/1 of the UaCPC, which reads as follows:

> 1. A search is conducted with the purpose of finding and fixing information on circumstances of commission of criminal offense, finding tools of criminal offense or property obtained as a result of its commission, as well as of establishing the whereabouts of wanted persons.

As a general rule, a search is executed on the basis of an investigating judge's ruling, which is issued on the basis of investigator's request approved by the public prosecutor, or by the request of the public prosecutor himself (art. 234/2). The content of any such request is regulated extensively in article 234/3.

The standard of proof which needs to be satisfied in order that the search request is allowed is defined by article 234/5, which reads as follows:

> 5. Investigating judge shall reject a request for search unless public prosecutor, investigator proves the existence of sufficient grounds to believe that:
>
> 1) a criminal offense was committed;
>
> 2) objects and documents to be found are important for pre-trial investigation;
>
> 3) knowledge contained in objects and documents being searched may be found to be evidence during trial;
>
> 4) objects, documents or persons to be found are in the home or any other possession of a person indicated in the request.

Procedure for execution of the search measure:

> Article 236. Execution of the ruling to authorize search of home or any other possession of a person
>
> Investigator or public prosecutor may execute the ruling to authorize a search of home or any other possession of a person. The victim, the suspect, defense counsel, representative, and other participants to criminal proceedings may be invited to attend. Whenever investigator, public prosecutor needs assistance in issues requiring special knowledge, they may invite specialists to participate in the search. The investigator, public prosecutor shall take adequate measures to ensure that persons whose rights and legitimate interests may be abridged or violated are present during such search.

Additional conditions / safeguards:

2. A search of home or other possession of a person based on investigating judge's ruling should be conducted in time when the least damage is caused to usual occupations of their owner unless the investigator, public prosecutor finds that meeting such requirement can seriously compromise the objective of the search.

3. Prior to the execution of investigating judge's ruling, the owner of home or any other possession or any other present individual in case of the absence of the owner, should be produced court's ruling and given a copy thereof. Investigator, public prosecutor may prohibit any person from leaving the searched place until the search is completed and from taking any action which impede conducting search. Failure to follow these requests entails liability established by law.

4. If no one is present in the home or other possession, the copy of ruling should be left visible in the home or other possession. In such a case, investigator, public prosecutor is required to ensure preservation of property contained in the home or any other possession and make it impossible for unauthorized individuals to have access thereto.

5. Search based on court's ruling should be conducted within the scope necessary to attain the objective of search. Upon decision of the investigator, public prosecutor, individuals present in the home or other possession may be searched if there are sufficient grounds to believe that they hide on their person objects or documents which are important for criminal proceedings. Such search should be conducted by individuals of the same sex.

6. During the search, investigator, public prosecutor shall have the right to open closed premises, depositories, objects if the person present during the search, refuses to open them, or if the search is conducted in the absence of persons specified in part three of this Article.

7. During the search, investigator, public prosecutor may conduct measurements, shoot pictures, make audio or video recording, draw plans and schemes, produce graphic images of the searched home or other possession of a person, or of particular objects, make prints and moulds, inspect and seize objects and documents which are important for criminal proceedings. Objects seized by law from circulation shall be subject to seizure irrespective of their relation to the criminal proceedings concerned. Seized objects and documents not included in the list of those directly allowed to be found in the ruling authorizing the search, and are not among objects withdrawn by law from circulation, shall be deemed provisionally seized property.

8. Persons who are present during the search have the right to make statements in the course of investigative (detective) action, such statements being entered in the record of search.

## 7.6 Real-time collection of traffic data and interception of content data

Ukrainian legislation does not define the term "traffic data" nor does it provide for separate measures of real-time collection of such data and interception of content data. Provisions of UaCPC, relevant in the context of Articles 20 and 21, are the following:

**Article 263. Collecting information from transport telecommunication networks**

1. Collecting information from transport telecommunication networks (networks which provide transmitting of any signs, signals, written texts, images and sounds or messages between telecommunication access networks connected) is a variety of

interference in private communication conducted without the knowledge of individuals who use telecommunication facility for transmitting information based on the ruling rendered by the investigating judge, if there is possibility to substantiate the facts during its conducting, which have the importance for criminal proceedings.

2. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics which will allow to uniquely identify the subscriber under surveillance, transport telecommunication network, and terminal equipment which can be used for interference in private communication.

3. Collecting information from transport telecommunication networks means the conducting using appropriate watch facility the surveillance, selection and recording information which is transmitted by an individual and have the importance for pre-trial investigation and also receiving, transformation and recording signals of different types which are transmitted by communication channels.

4. Collecting information from transport telecommunication networks is made by responsible units of the bodies of internal affairs and bodies of security. Managers and employees of telecommunication networks' operators shall be required to facilitate conducting the actions on collecting information from transport telecommunication networks, taking required measures in order not to disclose the fact of conducting such actions and the information obtained, and to preserve it unchanged.

**Article 264. Collecting information from electronic information systems**

1. Search, detection, and recording information stored in an electronic information system or any part thereof, access to the information system or any part thereof, as well as obtainment of such information without knowledge of its owner, possessor or keeper may be made based on the ruling rendered by the investigating judge, if there is information that such information system or any part thereof contains information of importance for a specific pre-trial investigation.

2. Obtainment of information from electronic information systems or parts thereof the access to which is not restricted by the system's owner, possessor or keeper, or is not related to circumventing a system of logical protection, shall not require permission of investigating judge.

3. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics of the electronic information system which can be used for interference in private communication.

**Article 265. Recording and preserving information obtained from communication channels through the use of technological devices and as a result of collecting information from electronic information systems**

1. Contents of information which is transmitted by persons via the transport telecommunication networks shall be stated in the record of conducting of the said covert investigative (detective) actions. If such information is found to contain knowledge of importance for a specific pre-trial investigation, the record should reproduce its respective part, and then public prosecutor shall take measures to preserve information obtained by monitoring.

2. Contents of information obtained as a result of monitoring an information system or any part thereof, shall be recorded on the appropriate medium by the individual who has been responsible for monitoring and who is required to ensure processing, preserving, and transmitting the information.

**Article 266. Examination of information obtained through the use of technological devices**

1. Information obtained through the use of technological devices shall be examined, if necessary, with participation of a specialist. Investigator analyzes contents of the information obtained and draws up a record thereof. In case of detection of information of importance for pre-trial investigation and trial, the record should reproduce the appropriate part of information and then public prosecutor takes measures to preserve information obtained.

2. Technological devices which have been used during the conduct of the said covert investigative (detective) actions, as well as original mediums for received information shall be preserved till the judgment takes legal effect.

3. Mediums and technological devices which helped obtain information may be the subject of examination by appropriate specialists or experts as prescribed in the present Code.

The aforementioned measures are executed on the basis of a judicial order. An on-going formal investigation is an absolute prerequisite. According to UaCPC 246.2, "investigative (detective) actions specified in Articles 260, 261, 262, 263, 264 (in part of actions based on the investigating judge's ruling) 267, 269, 270, 271, 272 and 274 of the present Code, as well as those the decision to conduct which are taken by investigating judge, shall be conducted exclusively in criminal proceedings in respect of grave crimes or crimes of special gravity". Procedural rules for conducting these types of measures are extensively covered by UaCPC 246 – 257.

Due to the fact that the new UaCPC was enacted during the preparation of this report, there were still many open questions as regards the application of its provisions in practice. For those reasons, we are not able to make a complete assessment of its provisions in the light of Article 15. As a preliminary conclusion, we believe that Ukraine is in line with article 21. In addition, since Ukraine uses a system of data retention, it might be argued that the purpose of Article 20 is also achieved.

## 7.7 Summary

| Article | Situation in the Ukrainian legislation | Recommendation |
|---|---|---|
| 16 | Not implemented by a preservation order. Seizure procedure can be used to secure data.<br>Not in line with Article 16. | Ukraine might wish to consider the implementation of a specific preservation order in the UaCPC. The subject-matter and the scope of such a measure should be defined in accordance with Articles 16 and 17 of the Convention. |
| 17 | Ukraine is not in line with Article 17. While Ukraine operates some data retention mechanism, rules on production of such data are not in line with the requirements of Article 17. | Ukraine might wish to consider the implementation of a specific preservation order in the UaCPC. The subject-matter and the scope of such a measure should be defined in accordance with Articles 16 and 17 of the Convention. |
| 18 | Ukraine is not in line with Article 17. While the provisions of UaCPC on provisional access to documents enable authorities to access stored computer data, they are substance rules on seizure and not the production order. | Ukraine might wish to consider the implementation of a specific preservation order in the UaCPC. The subject-matter and the scope of such a measure should be defined in accordance with Article 18. |

| | | |
|---|---|---|
| 19 | No specific provisions on computer-related search and seizure; "traditional" rules on search and seizure are used.<br><br>Conditions and safeguards used are described above (7.5). | Ukraine might wish to consider the implementation of specific provisions providing legal framework for computer-related search and seizure.<br>The situation envisioned in Article 19/2 should be addressed in specific provisions in UaCPC. Different options of seizing and similarly securing computer data, enumerated in Article 19/3, should be transposed in UaCPC.<br><br>Article 19/4 should be implemented, with appropriate conditions and safeguards.<br><br>Existing conditions and safeguards, mentioned above (7.5) should be kept in place. |
| 20 | More information needed to make conclusive assessment. | |
| 21 | No practical experience with the application of the measure. Requirements of Article 15 seem to be satisfied. | |