
2016/DGI/JP/3608
2018/DGI/JP/PMM 1963

5 May 2018

# Conditions and safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership

**Updated study prepared through country visits**

**October-November 2017, Eastern Partnership**

Prepared by Council of Europe experts
under the Cybercrime@EAP III Project

**www.coe.int/cybercrime**

Partnership for Good Governance

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

**Contact**

Cybercrime Programme Office of the

Council of Europe (C-PROC)

Email cybercrime@coe.int

**Disclaimer**

This review has been prepared by independent Council of Europe experts Marko Jurić and Marjan Stoilkovski with the support of the Cybercrime Programme Office of the Council of Europe.

This document has been produced as part of a project co-funded by the European Union and the Council of Europe. The views expressed herein can in no way be taken to reflect the official opinion of either party.

# Contents

1 Introduction ..... 6

1.1 Conditions and safeguards: What is required under Article 15 of the Convention on Cybercrime? ..... 6

1.1.1 Expedited preservation of stored computer data (Article 16) and expedited preservation and partial disclosure of traffic data (Article 17) ..... 8

1.1.2 Production order ..... 9

1.1.3 Search and seizure of stored computer data ..... 9

1.1.4 Real-time collection of traffic data ..... 10

1.1.5 Interception of content data ..... 11

2 Armenia ..... 16

2.1 Available statutes and other sources of information ..... 16

2.2 Expedited preservation of stored computer data ..... 16

2.3 Expedited preservation and partial disclosure of traffic data ..... 16

2.4 Production order ..... 17

2.5 Search and seizure of stored computer data ..... 17

2.6 Real-time collection of traffic data ..... 18

2.7 Interception of content data ..... 20

2.7.1 Legal basis ..... 20

2.7.2 The authorities' access to communications ..... 22

2.7.3 Authorization procedure ..... 23

2.7.4 Scope of application ..... 26

2.7.5 The duration of interception ..... 26

2.7.6 Procedures to be followed for storing, using, communicating and destroying the intercepted data ..... 27

2.7.7 Notification of interception of communications and available remedies ..... 28

2.7.8 Supervision ..... 29

3 Azerbaijan ..... 30

3.1 Available statutes and other sources of information ..... 30

3.2 Expedited preservation of stored computer data ..... 30

3.3 Expedited preservation and partial disclosure of traffic data ..... 30

3.4 Production order ..... 31

3.5 Search and seizure of stored computer data ..... 31

3.6 Real-time collection of traffic data....32
3.7 Interception of content data....33
3.7.1 Legal basis....33
3.7.2 The authorities' access to communications....34
3.7.3 Authorization procedure....34
3.7.4 Scope of application....36
3.7.5 The duration of interception....37
3.7.6 Procedures to be followed for storing, using, communicating and destroying the intercepted data....38
3.7.7 Notification of interception of communications and available remedies....39
3.7.8 Formalities....39
4 Belarus....40
4.1 Available statutes and other sources of information....40
4.2 General comment....40
4.3 Preliminary measures (articles 16 and 17 of the Convention)....40
4.4 Production order....40
4.5 Search and seizure of stored computer data....41
4.6 Real-time collection of traffic data....41
4.7 Interception of content data....42
5 Georgia....43
5.1 Available statutes and other sources of information....43
5.2 Expedited preservation of stored computer data....43
5.3 Expedited preservation and partial disclosure of traffic data....43
5.4 Production order....43
5.5 Search and seizure of stored computer data....45
5.6 Real-time collection of traffic data....47
5.7 Interception of content data....50
5.7.1 Legal basis....50
5.7.2 The authorities' access to communications....50
5.7.3 Authorization procedure....52
5.7.4 Scope of application....55
5.7.5 The duration of interception....56
5.7.6 Procedures to be followed for storing, using, communicating and destroying the intercepted data....58
5.7.7 Notification of interception of communications and available remedies....60
5.7.8 Supervision....61

6 Moldova ..... 63
6.1 Available statutes and other sources of information ..... 63
6.2 Expedited preservation of stored computer data ..... 63
6.3 Expedited preservation and partial disclosure of traffic data ..... 64
6.4 Production order ..... 65
6.5 Search and seizure of stored computer data ..... 67
6.6 Real-time collection of traffic data ..... 69
6.7 Interception of content data ..... 70
6.7.1 Legal basis ..... 70
6.7.2 Authorization procedure ..... 72
6.7.3 Scope of application ..... 73
6.7.4 The duration of interception ..... 74
6.7.5 Procedures to be followed for storing, using, communicating and destroying the intercepted data ..... 76
6.7.6 Notification of interception of communications and available remedies ..... 77
7 Ukraine ..... 78
7.1 Available statutes and other sources of information ..... 78
7.2 Expedited preservation of stored computer data ..... 78
7.3 Expedited preservation and partial disclosure of traffic data ..... 79
7.4 Production order ..... 79
7.5 Search and seizure of stored computer data ..... 83
7.6 Real-time collection of traffic data ..... 85
7.7 Interception of content data ..... 86
7.7.1 Legal basis ..... 86
7.7.2 Authorization procedure ..... 87
7.7.3 Scope of application ..... 89
7.7.4 The duration of interception ..... 89
7.7.5 Notification ..... 90

# 1 Introduction

## 1.1 Conditions and safeguards: What is required under Article 15 of the Convention on Cybercrime?

Convention on Cybercrime, in its Section 2 which covers procedural law, requires that its parties implement six specific procedural powers, namely expedited preservation of stored computer data (Article 16), expedited preservation and partial disclosure of traffic data (Article 17), production order (Article 18), search and seizure of stored computer data (Article 19), real-time collection of traffic data (Article 20) and interception of content data (Article 21). These procedural powers are necessary to effectively combat criminal offences by facilitating their detection, investigation and prosecution. On the other hand, application of these measures restricts (or interference with) fundamental human rights and freedoms, most importantly, with the right to private and family life, home and correspondence.

Therefore, pursuant to Article 15 of the Convention, it is necessary to ensure that these rights and freedoms are adequately protected. Article 15 reads as follows:

> *Article 15 – Conditions and safeguards*
>
> *1) Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.*
>
> *2) Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.*
>
> *3) To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.*

Article 15 seeks to ensure protection of fundamental rights and freedoms by mandating that each party to the Convention establishes in its domestic law that certain conditions and safeguards are to be applied in relation to the abovementioned procedural powers. These conditions and safeguards come from two sources:

a) Convention on Cybercrime itself. Namely, Convention stipulates that national law must:
    a. Incorporate the principle of proportionality – Article 15(1),
    b. Include "judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or

procedure" (all of this "as appropriate in view of the nature of the procedure or power concerned") – Article 15(2), and

c. Consider the "impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties" ("to the extent that it is consistent with the public interest, in particular the sound administration of justice") – Article 15(3).

b) International human rights treaties in general. For the European states, the most important instrument here is the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: ECHR). Since the provisions of this treaty are interpreted and upheld by the European Court of Human Rights (hereinafter: ECtHR), we must also, when applying Article 15 of the Convention on Cybercrime, consider requirements developed in its case-law.

As was explained above, measures in the Section 2 of the Convention on Cybercrime interfere with Article 8 of the ECHR. Pursuant to its Article 8(2), any interference with the right to private and family life, home and correspondence must (1) be in accordance with the law, (2) pursue one or more of the legitimate aims to which Article 8(2) refers, and must be necessary in a democratic society to achieve such aim. In this context, we note that there is no need to analyze separately the existence of legitimate aim, since measures in Section 2 of the Convention on Cybercrime above are used for detection, investigation and prosecution of criminal offences, which is recognized as a legitimate aim under Article 8(2) of the ECHR (prevention of disorder or crime).

Consequently, what is at stake here is whether national measures, as stipulated in law and as applied in practice, are in "in accordance with the law" and "necessary in democratic society". According to well-established case-law of the ECtHR, interference is "in accordance with the law" if it:

a) has some basis in domestic law, and it is

b) compatible with the rule of law. In order to be compatible with the rule of law, national law must meet the following quality requirements:

i. it must be accessible to the person concerned,

ii. it must be precise and foreseeable as to its effects. Regarding foreseeability, ECtHR stands on the position "*that domestic law must be sufficiently foreseeable in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are entitled to resort to measures affecting their rights under the Convention*".[1] But, foreseeability is not a synonym with absolute certainty. As the ECtHR has emphasized, "*many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice*".[2] Consequently, what is at stake here is the question of reasonable foreseeability. It is necessary that citizens are able to foresee to a reasonable degree, if need be with appropriate legal advice, in which circumstances relevant authorities can apply measures which correspond to those under Section 2 of the Convention on Cybercrime.

[1] Fernández Martínez v. Spain, ECtHR application no. 56030/07, para. 117.

[2] Silver and others v. The United Kingdom, ECtHR application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, para. 88.

iii. It must contain adequate safeguards against arbitrary application. In the case-law of the ECtHR, these safeguards have the most important role in the context of secret surveillance of communications (see below, 1.1.5).

### 1.1.1 Expedited preservation of stored computer data (Article 16) and expedited preservation and partial disclosure of traffic data (Article 17)

Article 16 of the Convention requires that its parties its Parties *"adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification"*.

There are two methods of implementing Article 16 (expedited preservation of stored computer data). The first, and the preferred one, is for a Party to introduce specific preservation order in its domestic legislation. The alternative, which is based upon the phrase "similarly obtain" in Article 16(1), is to use production order or search and seizure mechanism to expeditiously gain possession of data. While both methods can be used with equal efficiency, they are not the same in terms of compliance with fundamental human rights and freedoms.

Similarly, Article 17 requires of its parties to ensure (1) that "preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication", and (2) that competent authorities are empowered to request and receive "sufficient amount of traffic data to enable… [the identification of] the service providers and the path through which the communication was transmitted".

The main issue here is the application of the principle of proportionality. This principle, within the framework of procedural powers defined in the Convention on Cybercrime, entails balancing between different and competing options. However, such balancing is only possible if such options – i.e., different methods of achieving the same goal – exist in national legislation. Therefore, full implementation of *all procedural powers* envisaged in the Section 2 of the Convention on Cybercrime, including preservation orders defined in Articles 16 and 17, in itself enhances protection of human rights and freedoms. Namely, is preservation orders are implemented as a standalone measures in national legislation, law enforcement authorities have at their disposal less restrictive measure to be used when their primary goal is only to secure the data.

Moreover, using search and seizure with the sole aim of preserving data can have undue burden upon the rights, responsibilities and legitimate interests of third parties (data holders). And, pursuant to Article 15(3) of the Convention, these rights and interests need to be considered when assessing the impact of procedural powers.

When analyzing whether Articles 16 and 17 of the Convention are adequately implemented in national legislation, regarding requirements arising under Article 15, we take into account the following factors:

1) Whether articles 16 and 17 are implemented as standalone procedural powers in the national legislation;

2) Whether national law is precise and foreseeable. In particular, this requires that relevant notions be defined in domestic legislation (i.e., "traffic data");

3) Whether national law contains safeguards against arbitrary application;

4) Whether conditions defined in Article 16(2) of the Convention are implemented. This includes the following requirements:

    a. Preservation period is limited in time and clearly stipulated in the law.

    b. Preservation period does not initially exceed ninety days.

### 1.1.2 Production order

Article 18 of the Convention requires that its parties adopt such legislative and other measures as may be necessary to empower its competent authorities to order (1) production of computer data in general, and (2) production of subscriber information, in particular. This measure is to be used as Looking from the perspective of Article 15, the purpose of production order is to provide a less intrusive alternative to search and seizure.[3] As stated in the Explanatory report, "*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*".[4] In particular, the application of this measure is appropriate in situations where custodians of data are prepared to cooperate with authorities, but at the same time need to operate on the basis of clear legal duties and within foreseeable legal framework.[5]

When analyzing whether Article 18 of the Convention is adequately implemented in national legislation, with regard to requirements arising under Article 15, we take into account the following factors:

1) Whether Article 18 is implemented as standalone procedural power;

2) Whether national law is precise and foreseeable. In particular, this requires that relevant notions (i.e., "subscriber information") be adequately defined in domestic legislation;

3) Whether national law contains safeguards against arbitrary application.

    a. National law might exclude privileged data or information from the scope of production order,[6]

1) There is no consensus that judicial authorization should be required,[7]

### 1.1.3 Search and seizure of stored computer data

[3] Explanatory report, para 170 – 171.
[4] Explanatory report, para 170.
[5] See Explanatory report, para 171.
[6] Explanatory report, para 174.
[7] See extensively practices of different countries in Rules on obtaining subscriber information, Report adopted by the T-CY at its 12th Plenary (2-3 December 2014).

In essence, Article 19 of the Cybercrime Convention requires that every Party adopts legislative and other measures necessary to empower the competent authorities to (1) conduct measure of search of similar accessing, (2) expeditiously extend such measure to linked systems, (3) seize computer system, mediums or data and (4) order any person who has knowledge or information necessary to conduct search to provide them.

For the purposes of assessing the compliance with Article 15, the following list of conditions and safeguards needs to be taken into account.

1) Compliance with the rule of law:

    a. Search and seizure powers are defined by national legislation (there is adequate legal basis),

    b. National law is accessible,

    c. National law is precise and foreseeable. In particular, we need to assess whether possible notions of traditional search and seizure ("objects" or "documents") are sufficiently clear if applied to computer related search, from the perspective of legal certainty,

    d. National law contains safeguards against arbitrary application.

2) Necessity requirements:

    a. National law should require existence of adequate grounds justifying application of search and seizure measure,

    b. National law should stipulate that search and seizure is subject to judicial or other independent supervision. Procedure for search in urgent circumstances must also ultimately result in timely judicial supervision,

    c. National law should stipulate that legally privileged information are exempted from the scope of this measure,

    d. We will consider implementation of all seizure options defined in Article 19(3) of the Convention as beneficial in the light of Article 15, since it broadens the possibility for law enforcement and enables the use of less-restrictive measure.

### 1.1.4 Real-time collection of traffic data

We start from the premise that in most EAP countries exists technical possibility of real-time collection of traffic data. In such circumstances, in order to conclude that national implementation of Article 20 is adequate in the light of conditions and safeguards (Article 15), we need to establish that the following conditions are met:

1) Compliance with the rule of law:
    a. Procedural powers are defined by national legislation (there is adequate legal basis),
    b. National law is accessible,
    c. National law is precise and foreseeable. This includes the requirement that relevant notions ("traffic data") are precisely defined in law.
    d. National law contains safeguards against arbitrary application.

2) Necessity requirements:
    a. National law should require existence of adequate grounds justifying application of this measure,
    b. National law should stipulate that this measure is subject to judicial or other independent supervision,
    c. In general, it is necessary to reach conclusion that legal framework regulating real-time collection of traffic data computer data, as applied in practice, provides adequate protection against arbitrary application.

### 1.1.5 Interception of content data

Secret surveillance of communications is a necessary tool for law enforcement authorities of every country. It enables them to fulfil their tasks within the society, namely to protect national security and investigate and prosecute serious criminal offences. But, if abused, secret surveillance "*may undermine or even destroy democracy under the cloak of defending it*".[8] Therefore, the main challenge here is how to design a legal and technical system which enables relevant authorities to fulfil their tasks, while at the same time minimizing the risk of potential abuses of such system.

There is no denying that interception of content data is the most intrusive procedural power in the Convention on Cybercrime. In relation to surveillance of communications in general, this was long ago recognized by the European Court for Human Rights (ECtHR). For instance, it was emphasized in Kruslin v France (1985)[9] that "*tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence…*". For this reason, the ECtHR has consistently required that interception of communications be based on "*a "law" that is particularly precise*". As elaborated by the Court, "*it is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated*".[10] More precisely, "*the domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*".[11]

Moreover, the ECtHR seeks to limit discretion of national authorities. As explained in *Zakharov v Russia* and many other cases, "*since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference*".[12] In order to limit the power which might be exercised by national authorities, and its potential abuse, the ECtHR has developed *list of minimum safeguards* that must be set in national law: the nature of offences which may give rise to an interception order; definition of the categories of people liable to have their communications intercepted; duration of interception; procedure to be followed for examining, using and

[8] Zakharov, para. 232.
[9] Kruslin v France, ECtHR application no. 11801/85, para 33.
[10] Kruslin, para 33; Zakharov v. Russia, para. 229.
[11] Zakharov v Russia, para 229, Association for European Integration and Human Rights and Ekimdzhiev, para 75.
[12] Zakharov, para 230.

storing the data obtained; precautions to be taken when communicating the data to other parties; circumstances in which recordings may or must be erased or destroyed.[13]

In particular, it is necessary to ensure in every case that interference with fundamental rights and freedoms is "necessary in a democratic society". Requirement of necessity must be satisfied on both the legislative level and in its application in practice.[14]

For the purposes of this report, we are going to compare national legislation of the project countries with the following list of requirements.

### 1.1.5.1 Legal basis

In the context of interception of communications, our first task is to verify whether there is a proper legal basis for such measure in the national legislation. This means that national law must contain specific legal power which enables competent authorities to intercept communications' content data. Moreover, as already elaborated above, interception of communications is a serious restriction of the right to private life and consequently must be based on a legal framework that is *particularly precise*. Noting that in most project countries interception of communications is a special investigative action, we must analyse the relation between statutes which regulate criminal procedure and those which cover special investigative measures. In particular, we seek to establish whether interception is possible only under the conditions stipulate in statutes on criminal procedure, or both. If the latter is the case, then we also need to establish whether both statutes implement proper conditions and safeguards.

### 1.1.5.2 Authorization procedure

According to the ECtHR, authorization procedures in national law must ensure "that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration". In analysing these procedures, we must consider (1) which authority is competent to authorise the surveillance according to national legislation, (2) its scope of review and (3) the content of the interception authorisation.[15]

In most countries, authorization of interception is done by the courts. However, ECtHR has held that "authorising of telephone tapping by a non-judicial authority may be compatible with the Convention, provided that that authority is sufficiently independent from the executive".[16] Moreover, it is ordinary legislative practice to allow, in cases of urgency, that interception of communications be initiated without court authorization. Such practice is compatible with the Convention, provided that subsequent judicial review is done, and that other appropriate safeguards are implemented.

Regarding the authorization authority's scope of review, the ECtHR held that this authority must be capable of verifying:

[13] Zakharov v Russia, para 231.
[14] Zakharov, para 231.
[15] Zakharov v. Russia, para 257.
[16] Zakharov v. Russia, para 257 and other cases quoted there.

1) "the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures"

2) "whether the requested interception meets the requirement of "necessity in a democratic society", … including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means".[17]

Content of authorization order

Finally, ECtHR has held that interception authorisation "must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information".[18]

### 1.1.5.3 Scope of application of interception measures

Scope of application of interception measures must be limited. There are three dimensions of these limitations.

Firstly, national law should stipulate that interception can be used only in relation to a limited number of criminal offences. This follows clearly from the Article 21 of the Convention, principle of proportionality and the case-law of the ECtHR. In this context, scope of application of interception measure can be restricted for instance by linking its application to specific categories of serious crimes (i.e., according to their gravity, if such classification is recognized in national law) or by enumerating specifically, in the procedural law, which criminal offences can trigger the application of interception.

Secondly, national law must define categories of people liable to have their communications intercepted (e.g., suspect, defendants, etc.). In this context, it is important that national law avoids vague notions such as ""a person who may have information about a criminal offence", "a person who may have information relevant to the criminal case",[19] "other person involved in a criminal offence",[20] etc.

### 1.1.5.4 The duration of interception

There are no uniform standards under the Convention on Cybercrime and the ECHR prescribing maximum overall duration of interception. According to ECtHR's case law, "it is not unreasonable to leave the overall duration of interception to the discretion of the relevant domestic authorities which have competence to issue and renew interception warrants, provided that adequate safeguards exist, such as a clear indication in the domestic law of the

[17] Zakharov v. Russia, para 260 and other cases quoted there.
[18] Zakharov v. Russia, para 264 and other cases quoted there.
[19] Zakharov v Russia, para 245.
[20] Iordachi and Others v. Moldova, para 44.

period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled".[21]

### 1.1.5.5 Procedures to be followed for storing, using, communicating and destroying the intercepted data

According to the case-law of the ECtHR, national law should contain "clear rules governing the storage, use and communication of intercepted data". [22] In this context, it is not possible to give precise list of requirements which need to be satisfied by national legislation. Instead, it is necessary that national law contains sufficient safeguards which can minimise the risk of unauthorised access or disclosure.[23] In particular, national law should prescribe that any data which are not relevant to the purpose for which they have been obtained must be destroyed immediately.[24]

### 1.1.5.6 The authorities' access to communications

In its case-law, the ECtHR uses special scrutiny in those cases where "the security services and the police have the technical means to intercept mobile telephone communications without obtaining judicial authorisation, as they have direct access to all communications and as their ability to intercept the communications of a particular individual or individuals is not conditional on providing an interception authorisation to the communications service provider" According to the Court, "the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception".

According to the ECtHR, systems which enable direct access to communication infrastructure are "particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great".

### 1.1.5.7 Notification of interception of communications and available remedies

According to the ECtHR, notification of interception of communications "is inextricably linked to the effectiveness of remedies before the courts".25 In this context, the ECtHR notes that "it may not be feasible in practice to require subsequent notification in all cases", for instance, if the danger which gave rise to interception is still present, or notification would jeopardise the purpose of interception, or it would "reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents". But, "as soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should … be provided to the persons concerned".

[21] Zakharov v. Russia, para 250 and other cases quoted there.
[22] Zakharov v. Russia, para 253 and other cases quoted there.
[23] Zakharov v. Russia, para 253 and other cases quoted there.
[24] Zakharov, para 253-256.
[25] Zakharov v. Russia, para 286 and other cases quoted there.

In particular, "absence of a requirement to notify the subject of interception at any point was incompatible with the Convention, in that it deprived the interception subject of an opportunity to seek redress for unlawful interferences with his or her Article 8 rights and rendered the remedies available under the national law theoretical and illusory rather than practical and effective. The national law thus eschewed an important safeguard against the improper use of special means of surveillance".

On the contrary, "in the case of Kennedy the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception subject that there had been an interception of his or her communications".

# 2 Armenia

## 2.1 Available statutes and other sources of information

This part of the Report is based on the following sources:

1. Armenian Code on Criminal Procedure (hereinafter: AmCPC),
2. Armenian Law on Operative-Intelligence Activity (hereinafter: AmLOIA),
3. Information provided by national stakeholders during the mission to Armenia organized by the Council of Europe's Cybercrime Programme Office and held in Yerevan on October 16 and 17, 2017.

## 2.2 Expedited preservation of stored computer data

Armenian legislation does not recognize expedited preservation of stored computer data (Article 16 of the Convention) as a standalone measure. To be sure, there are many sector-specific regulations which mandate retention of certain types of documents, including computer data (i.e., in the banking sector, CCTV recordings, etc.). However, there is no generally applicable provision which would enable expedited preservation of computer data in general.

In these circumstances, search and seizure is a default measure to secure computer data in the context of criminal investigations. While this approach might satisfy the needs of law enforcement authorities (if it is efficient enough), it is not completely satisfactory when protection of fundamental human rights and freedoms is at stake. As we explained in the introduction, the main issue here is the application of the proportionality principle. In short, we hold that full implementation of *all procedural powers* envisaged in the Section 2 of the Convention on Cybercrime (including preservation orders) contributes *per se* to the protection of fundamental human rights and freedoms. This is so because it enables the broadest application of the proportionality principle. Namely, if preservation orders are implemented as standalone measures, law enforcement authorities have at their disposal less restrictive means to be used when the primary goal is only to secure the data. Therefore, in the context of Armenian legislation, we consider that implementation of standalone preservation orders would enable (where appropriate) the use of less intrusive procedural powers, and would therefore represent a significant step forward towards the full compliance with Article 15 of the Convention.

## 2.3 Expedited preservation and partial disclosure of traffic data

Regarding Article 17 (expedited preservation and partial disclosure of traffic data), it first needs to be noted that there is no differentiation in the AmCPC between different types of computer data (i.e., subscriber information, traffic data and content data). Also, Armenian legislation does not include any provisions designed specifically for preservation of traffic data. Moreover, the situation regarding retention of traffic data remains unclear. According to explanations provided by national stakeholders, communication service providers do retain some traffic data, for various purposes, as a matter of their internal practice. In these cases, retention periods vary, according to the needs and policies of the provider in question.

However, this is not an optimal solution, neither for law enforcement authorities nor for the public. Therefore, we consider that implementation of precise and foreseeable rules regarding preservation of traffic data and/or their retention would contribute significantly to the quality of Armenian legislation.

## 2.4 Production order

There are no specific provisions with the scope and purpose corresponding to Article 18 of the Convention on Cybercrime in the Armenian legislation. In such circumstances, it is necessary for Armenian authorities to rely upon the general rules of seizure in order to secure possession of computer data. In this context, Article 228(6) of the AmCPC stipulates that "*when conducting a seizure, after presenting and announcing the warrant, the investigator proposes to hand over the articles and documents subject to seizure of one's own accord, in case of refusal, compulsory seizure is done*". Also, as explained below, the scope of the term "document" is broad enough to include also computer data. Therefore, it can be said that the main purpose of Article 18 – to provide an alternative to the use of coercive measure – can also be achieved on the basis of the AmCPC.

On the other hand, it is also true that there is no differentiation in the AmCPC between different categories of data, namely subscriber information, traffic data and content data. In such circumstances, it cannot be said that Armenian legislator succeeded in achieving full compliance with Article 15.

## 2.5 Search and seizure of stored computer data

There are no provisions in the AmCPC which would create specific legal framework for computer-related search and seizure. In such circumstances, traditional powers of search and seizure of tangible objects are used as a legal basis giving effect to Article 19 of the Convention on Cybercrime. These powers are regulated in Chapter 31, Articles 225 – 231 of the AmCPC.

As a general rule, pursuant to Article 225(1) of the AmCPC, search can be conducted when 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*". Where ordinary search and seizure are used in computer-related circumstances, the first issue which usually arises is whether notions used in the law are adequate to describe intangible object – computer data. In the context of the AmCPC, we need to verify whether the notion of "other items or documents" can include stored computer data. In this context, Article 225(1) needs to be interpreted in line with Article 122(1), which stipulates that "*any record registered on a paper, electronic or other media made in verbal, digital, graphic or other sign/symbol form which can provide information relevant to the criminal case is a document*". Since the notion of document therefore includes records in electronic/digital form, we conclude that Armenian law is sufficiently precise and foreseeable in prescribing that computer data can be the object of search and seizure.

Article 19(3) of the Cybercrime Convention, which provides for several different modalities of seizing computer data, is not implemented adequately in Armenian CPC. According to the provisions of this code, it is stipulated only that when it is necessary to seize "*articles and*

*documents significant for the case, and provided it is known for sure where they find themselves and in whose possession, the investigator conducts seizure*".[26] According to explanations given by national stakeholders, in practice law enforcement authorities can and do use less intrusive methods of seizure (i.e., making and retaining a copy of stored computer data), instead of more intrusive ones (seizing computer equipment). This is also supported by the provision of the AmCPC which stipulates that "*when conducting a search the investigator or the expert can use technical devices…*".[27] Therefore, there seems to be no dispute whether current legal framework enables the use of less intrusive methods of seizure. But, on the basis of the quality of law requirement, which arises under the ECHR, case-law of the ECtHR as well as the Convention on Cybercrime itself, this should also be adequately reflected in the text of the AmCPC. In current situation, law enforcement authorities and the courts have unfettered discretion over the method of conducting seizure. This should be avoided. From the perspective of Articles 19(3) and 15 of the Cybercrime Convention, adequate solution would be the one where different modalities of conducting seizure would be clearly defined in the law, and where investigators, prosecutors and the courts would be under a legal obligation to use the method which is (in particular circumstances) the least restrictive.

From a formal viewpoint, search is executed on the basis of a court order.[28] In order for such order to be issued, there has to exist an open criminal case. Moreover, search and seizure warrant can be issued if there are sufficient grounds to suspect that objects significant for the case can be found in some premises, some other place or in possession of some person.[29] All of these conditions are important safeguards against arbitrary application of the law.

Additionaly, some other formalities are also envisaged in the AmCPC. These include the obligatory presence of attesting witnesses, as well as of some other persons in specific circumstances, who should be present when search and/or seizure is conducted.[30] Moreover, prior to conducting search or seizure, investigator should present the search warrant to the person against whom the measure is directed.[31] Next, investigators are under obligation to keep confidential facts established during search / seizure, as well as details regarding private life of the searched persons.[32] Finally, detailed search protocol has to be made, and later on given to relevant persons.[33]

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

In Armenian legislation, no distinction is made between the real-time collection of traffic data and interception of content data. According to explanations given by national authorities, both

[26] Article 226(1) of the AmCPC.
[27] Article 228(3) of the AmCPC.
[28] AmCPC, Article 225(3).
[29] AmCPC, Article 225(1-3).
[30] AmCPC, Article 227.
[31] Article 228(1) of the AmCPC.
[32] Article 228(4) of the AmCPC.
[33] Articles 230 and 231 of the AmCPC.

of these measures can be undertaken on the basis of Chapter 33 of the AmCPC and Article 26 of the AmLOIA.

The main difficulty here is that Chapter 33 of the AmCPC (articles 239, 240 and 241) does not define precisely the scope of procedural powers in relation to traffic data. In particular, while Article 239 makes reference to "mail or other correspondence, mail, telegrams and other communications", there is no mention here of traffic data or any similar notion which could be used to describe the same set of data. The same is true for paragraph 3 of this article, which stipulates that "*the correspondence which can be arrested, in particular, concerns the following items: letters, telegrams, radiograms, parcels (printed matter), cases, post containers, transmissions, fax and e-mail messages*". Moreover, the language of this provision implies that Article 239 is applicable primarily to content data. This follows from its paragraph 1, which mentions communications "sent by the suspect or the accused or to them by other persons". Similarly, Article 241 of the AmCPC prescribes so-called "supervision and recording" over telephone and other conversations. Once again, it is not clear from the law whether this provision covers only content data, or whether it includes also traffic data. In any event, as already noted above, one of the main shortcomings of the AmCPC in general is the lack of differentiation between various categories of data (subscriber information, traffic data and content data). In this context, it is necessary that Armenian legislator draws a clear distinction between measures corresponding to Articles 20 and 21 of the Convention, and introduces precise and foreseeable definitions for all necessary notions (most importantly in this context, traffic data).

Unlike with the AmCPC, some differentiation between various categories of data can be found in the AmLOIA. In particular its Article 26, which deals with wiretapping, prescribes 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.*

Pursuant to this provision, wiretapping is defined as "secret control over the phone conversations, including internet conversations and electronic communications". It also covers collection of information which essentially fall within the scope of traffic data, in accordance paragraphs 1(b-d), 2(b) and 3(a-c). Therefore, AmLOIA enables collection of traffic data under the same set of conditions as interception of content data (paragraphs 1(a), 2(a) and 3).

In these circumstances, it must be concluded that Article 15 is not given adequate effect vis-à-vis real-time collection of traffic data in the AmCPC, since there is no adequate legal basis for this measure in the AmCPC, and since, in any event, AmCPC is not sufficiently precise and foreseeable here. On the other hand, AmLOIA makes it sufficiently predictable which information can be collected by law enforcement authorities.

Moreover, in terms of conditions and safeguards, it must be noted once again that Article 26 of the AmLOIA applies without difference to content data and other information about communication. Consequently, the same set of legal rules is applied here. Conditions and safeguards applicable to monitoring of traffic data are therefore the same as the ones applicable to interception of content.

## 2.7 Interception of content data

### 2.7.1 Legal basis

In Armenian legislation, there are two statutes that regulate interception of content data: AmCPC and AmLOIA. We note at the beginning that these two statutes do not have the same scope (in relation to interception measures). Namely, AmLOIA contains independent legal grounds for interception.[34] In other words, it is possible to order interception only on the basis of AmLOIA, without simultaneously applying AmCPC. This does not necessarily mean that Armenian legislation is inadequate. However, it requires us to verify whether conditions and safeguards are adequately set in both statutes which are relevant here (AmCPC and AmLOIA). Different approach can be seen in other project countries, i.e. Moldova and Georgia. For instance, Moldovan law stipulates precisely that certain operative-investigative activities (including interception) can be performed only under the Criminal Procedure Code of the

[34] Article 4 of the AmLOIA.

Republic of Moldova.[35] Similar solution can be found in Article 7(3) of the Georgian Law on Operative Investigatory Activities.[36]

There are two measures which include surveillance of communication's content in the Chapter 33 of the AmCPC: (1) so-called "*monitoring of correspondence, mail, telegrams and other communications*" (Article 239) and (2) "*supervision over conversation*" (Article 241). There is a slight ambiguity in the scope of these provisions. Namely, it seems that the purpose of the first measure is to enable monitoring of those communications where there is a tangible object of communication, whilst the second one concerns remote communication ("conversation") by some technical means. However, the distinction between these powers is not completely clear, especially where computer-related communications are concerned. While it would be expected that Article 239, which regulates "*monitoring of correspondence, mail, telegrams and other communications*" pertains to tangible objects, this is not completely true. Pursuant to paragraph 3 of this article this measure covers "*letters, telegrams, radiograms, parcels (printed matter), cases, post containers, transmissions, fax and* ***e-mail messages***" (emphasis ours). In this context, we note that Article 239 can hardly be applicable to e-mail communication. For instance, it is prescribed in its paragraphs 4 and 5 that "decision on the monitoring of correspondence is sent to the appropriate post office director for whom it is mandatory", and that "the director of the post office withholds the correspondence indicated in the decision of the investigator and advises the latter about that". These procedures can hardly be relevant when interception of e-mail communication is at stake. More importantly, we do not see any practical or legal reason to treat surveillance of e-mail communication differently than other form of electronic communications, e.g. instant messaging or other forms of internet communication. For instance, in Ukrainian Criminal Procedure Code similar measure is limited to "material mediums for exchange of information", and surveillance of telecommunications is subject to a different procedural power.[37] Consequently, we believe that Armenian legislator should follow the same approach and draw a clear distinction between monitoring of communications in tangible form and those which are transmitted by telecommunication / electronic communication means.

On the other hand, Article 241 of the AmCPC is more specific since it covers supervision over *conversations*. It follows from the text of this provision that conversations in question are those by telephone or "other means of communication". Consequently, interception of content data using some other applications (instant messaging, internet telephony) could fall within the scope of Article 241. In this context, we believe that foreseeability of Article 241 should be improved by defining more specifically which communications fall within the notion of "other means".

Finally, there are two operational-intelligence measures, defined in the AmLOIA, which correspond to powers defined in the AmCPC: (1) interception of correspondence, postal, telegram and other communications (Article 25 of the AmLOIA) and (2) wiretapping (Article 26 of the AmLOIA). In general, Article 25 of the AmLOIA corresponds broadly to AmCPC Article 239, and Article 26 of the AmLOIA is related to Article 241 of the AmCPC.

In comparison with the AmCPC, AmLOIA is more precise since it deals in its Article 26, in the context of "wiretapping", with "monitoring of conversations, including internet telephone

[35] See chapter 6.7.1 below.
[36] See chapter 5.7.1 below.
[37] See chapter 7.7.1 below.

conversations and electronic communication", and more specifically "fixed telephony", "mobile telephony" and "Internet communication". Moreover, unlike AmCPC, AmLOIA seems to treat e-mail communication ("electronic messages transferred over the Internet") under the same rules as telephone conversations (that is, under Article 26).

Nevertheless, there is once again some vagueness regarding the scope of "interception of correspondence, postal, telegram and other communications" (Article 25 of the AmLOIA). Firstly, it is not sufficiently foreseeable what might be considered "other communications" for the purposes of this provision. Moreover, it is stipulated in Article 37(3) that the motion to conduct operational intelligence measure referred to in point 11 of part 1 of Article 14(1)(11), which is "interception of correspondence, postal, telegram and other communications", must include

> *"the postal address or electronic address to be intercepted, keywords or key phrases representing search interest (for interception of mailing and other types of communication in case of absence of postal or electronic address or of keywords or key phrases representing search interest, sample of handwriting or other specifics, sufficient for identification of the person, whose correspondence, postal, telegram or other types of communication shall be intercepted, may be submitted.*

Obviously, AmLOIA (like AmCPC) does not contain a clear distinction between monitoring of communications in tangible form and those which are transmitted by telecommunication / electronic communication means. Consequently, we propose that this shortcoming also be addressed in future.

### 2.7.2 The authorities' access to communications

In Armenian legislation, interception of communications falls under the competence of "service functioning within the system of the republican national security body of the Republic of Armenia". Pursuant to Article 9 of the AmLOIA,

> *1. Conducting of operational intelligence measure of wiretapping shall, in accordance with the procedure prescribed by this Law, be ensured only by the service functioning within the system of the republican national security body of the Republic of Armenia (hereinafter referred to as the Service) upon motion of the body authorised to conduct such operational intelligence measure.*

Moreover, AmLOIA stipulates that "the Service provides telecommunication operators with necessary operational-technical facilities to carry out operational intelligence measure of wiretapping by the bodies authorised by this Law".[38] Similarly, it is prescribed in Article 31(5) of the AmLOIA that

> *5. When carrying out operational intelligence measures laid down in point 12 of part 1 of Article 14 of this Law, telecommunication and postal organisations shall upon the request of the Service provide technical facilities and create other conditions necessary for carrying out operational intelligence measures.*

[38] AmLOIA, Article 9(5).

> *6. When carrying out operational intelligence measures laid down in point 11 of part 1 of Article 14 of this Law, telecommunication and postal organizations shall, upon the request of national security bodies as well as the police and penitentiary authorities, in cases laid down in part 3 of this Article, provide technical facilities and create other conditions necessary for carrying out operational intelligence measures.*

Therefore, it seems evident that Armenian legislation creates certain obligations for providers, including, inter alia, provision of "technical facilities" and creating "other conditions necessary for carrying out operational intelligence measures". While the exact scope of obligations under this provision is for obvious reasons classified and therefore not available to us, it seems reasonable to conclude that there are some possibilities of direct access to communications networks in Armenia. Since, as noted by the ECtHR and explained in the introduction, systems which enable direct access to communication infrastructure are "particularly prone to abuse", it is of fundamental importance that national legislation ensures that all necessary and appropriate safeguards against arbitrariness and abuse are implemented. The effectiveness of those safeguards will be analysed below.

## 2.7.3 Authorization procedure

### 2.7.3.1 Authority competent to authorize interception

Pursuant to Article 241(1) of the AmCPC, decision to "permit the supervision and recording of … conversations" is made by the court, upon the grounded motion made by the investigator. This is in line with general principles of the AmCPC, which stipulates that "*everyone has the right to confidentiality of correspondence, telephone conversations, mail, telegraph and other communications*". According to the law, limitations of this right "*may be ordered in the course of criminal proceedings only upon a decision of the court and in the manner prescribed by law*".[39] There are numerous other provision in the AmCPC which stipulate that interference with constitutional rights and freedoms fall within the domain of judicial competence.[40]

On the other hand, we note that Article 239(1) which covers "monitoring of correspondence, mail, telegrams and other communications", including e-mail, stipulates that "the investigator can make a grounded decision to impose monitoring on the correspondence of these people". In such circumstances, it remains ambiguous whether monitoring of correspondence can be imposed solely on the basis of investigator's decision, or whether other provisions of the AmCPC and the AmLOIA, which call for judicial authorization, take precedence.[41] We believe that this issue should be addressed by Armenian legislator, and that AmCPC should prescribe without any ambiguity that all measures which restrict privacy of communications must be undertaken solely on the basis of judicial authorization.

Similarly, AmLOIA makes it clear that operational-intelligence measure of wiretapping can be made only under judicial supervision and with a prior court order.[42] The same requirement is applicable in relation to "interception of correspondence, postal, telegram and other communications", pursuant to Article 34(1) of the AmLOIA.

[39] Article 14 of the AmCPC.
[40] See *inter alia* AmCPC Article 278, 279, 280 etc.
[41] AmLOIA, Article 34(1).
[42] AmLOIA, Article 32(1)

By way of exception, "*where delay in conducting operational intelligence measures as prescribed by this Article may result in an act of terrorism or in events or actions threatening the state, military or environmental safety of the Republic of Armenia*", it is possible to initiate wiretapping without the court order.[43] In those circumstances, court order needs to be presented within 48 hours.

Moreover,

> *"In case of failure to submit to the Service the extract of the decision of the court within 48 hours as provided for in part 3 of this Article or in case of submitting the decision of the court denying authorisation to carry out operational intelligence measures laid down in this Article, such activity shall be immediately terminated, and information and materials already acquired shall be immediately destructed by the authority carrying out the measure. The head of the Service immediately reports to the President of the Republic of Armenia on each case laid down in this part".*[44]

Similar urgent authorization procedure is applicable also in relation to "interception of correspondence, postal, telegram and other communications", pursuant to Article 34(3) of the AmLOIA:

> *3. If the delay in carrying out operational intelligence measures may result in an act of terrorism or events or actions threatening the state, military or environmental safety of the Republic of Armenia, and for carrying out of which court's authorisation is mandatory under this Law, implementation of such measures within 48 hours is permitted based on the decision of the head of operational intelligence body through notifying the court, as prescribed by the Criminal Procedure Code of the Republic of Armenia. If the court does not deem the grounds for conducting operational intelligence measures to be sufficient, the conducting thereof is immediately terminated and the information and materials acquired as a result thereof are immediately destructed. Otherwise the court issues a decision authorising to carry out operational intelligence measures.*

In general, we consider that this procedure provides sufficient safeguards against arbitrary application. Firstly, subsequent judicial authorization is required. Secondly, if such subsequent authorization is not granted, interception must be terminated, and all information and materials destroyed immediately.

### 2.7.3.2 Authorizing authority's scope of review

Next, we look at the authorization authority's scope of review. As explained in the introduction, the ECtHR has held that this authority it must be capable of verifying (1) the existence of a reasonable suspicion against the person concerned, and (2) whether the requested interception meets the requirement of "necessity in a democratic society". The

[43] AmLOIA, Article 32(2).
[44] AmLOIA, Article 32(3).

purpose of this is to ensure that "*secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration*".[45]

Firstly, AmCPC stipulates in its Article 241(1) that supervision over conversation can be ordered by the court "*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*". Similarly, Article 239 which covers "monitoring of correspondence, mail, telegrams and other communications", including e-mail, stipulates that it this measure is applicable "*when there are sufficient grounds to believe that there is probatory value data in the mail or other correspondence… sent by the suspect or the accused or to them by other persons…*". However, second requirement (that authorizing body, in this case the court, verifies whether the requested interception meets the requirement of "necessity in a democratic society") is not present in the AmCPC. This is a significant shortcoming in the law, and should be addressed by the legislator as soon as possible. On the other hand, provisions of AmLOIA are adequate, since it stipulates in Article 31(4) that

> "*Operational intelligence measures* [of interception of correspondence and other communications, as well as wiretapping] *may be conducted only … if there is substantiated evidence that it is impossible for the body carrying out operational intelligence activity in any other manner to acquire information required for the fulfilment of the tasks conferred thereon by this Law".*

Unlike the AmCPC, AmLOIA stipulates precisely that interception of communications and wiretapping can be applied only if it is impossible to achieve the aim pursued by any other means.

### 2.7.3.3 Precision of interception order

Finally, ECtHR has held that interception authorisation "must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information".[46]

In this context, we note that the AmCPC requires that court's decision in cases under Article 241 must contain "the surnames and names of the persons whose conversations are subject to supervision".[47] Similar requirement is contained in Article 239(2) of the AmCPC, dealing with "monitoring of correspondence, mail, telegrams and other communications".

Moreover, AmLOIA stipulates in its Article 32(1) that extract of court's decision, submitted to Service tasked with wiretapping, must contain "only the line subject to wiretapping". Also, we note that Article Article 38(2)(2) stipulates that "operational intelligence body is not entitled to perform actions that are not provided for in a decision on conducting operational intelligence measure". Unfortunately, we were not able to identify other provisions of the AmLOIA which would define more precisely the content of interception orders. Consequently, we propose that this issue be addressed in future amendments to the AmLOIA.

[45] Zakharov v Russia, ECtHR app. no. 47143/06, para 257.
[46] Zakharov v. Russia, para 264 and other cases quoted there.
[47] AmCPC, Article 241(2).

### 2.7.4 Scope of application

As explained in the introduction, international law requires that domestic legislation restricts the application of interception measures in relation to a limited range of serious criminal offences. Moreover, it requires also that national law defines with precision categories of people liable to have their communications intercepted.

First of these conditions (limitation vis-à-vis categories of crimes) is not present in the Armenian legislation. This is a serious shortcoming in the law and should be addressed as soon as possible. On the other hand, AmLOIA stipulates in Article 31(4) that "*Operational intelligence measures* [of interception of correspondence and other communications, as well as wiretapping] *may be conducted only in case the person, with respect to whom the measure is to be conducted, is suspected of committing a grave and particularly grave crime…"*, which is, in general, an adequate safeguard.

Secondly, application of Article 241(1) of the AmCPC is limited to communications of a suspect or accused. Similarly, Article 31(4) of the AmLOIA is applicable against a person who is "suspected of committing a grave and particularly grave crime". Consequently, we conclude that Armenian legislation limits, in a foreseeable manner, categories of people liable to have their communications intercepted.

Finally, we note that certain communications are exempted from the scope of interception measures. Pursuant to Article 31(7) of the AmLOIA, "*It is prohibited to carry out operational measures* [of interception of correspondence and other communications, as well as wiretapping] *if a person, with respect to whom the measure concerned is to be carried out, is communicating to his/her lawyer. Information containing lawyer's secret - obtained in the process of carrying out operational intelligence measures referred to in points 8, 11 and 12 of part 1 of Article 14 by reasons not related to the objective of carrying out operational intelligence - shall be immediately destructed"*. This also represents an important safeguard against potential abuses.

### 2.7.5 The duration of interception

In the AmCPC, duration of "supervision over conversation" is limited pursuant to its Article 241(4). According to this provision,

> *"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".*

On the other hand, no such limitation is used in relation to "monitoring of correspondence, mail, telegrams and other communications" (which includes e-mail). In this context, we note that a decision to impose such monitoring must contain, *inter alia*, "the period of monitoring". However, this period is not limited in any way in the AmCPC. This is a serious shortcoming of the law and should be corrected as soon as possible.

In the same context, AmLOIA stipulates in its Article 39(1) that

> *"the term of the decision on conducting operational intelligence measures shall be counted beginning from the date of its adoption and shall not exceed 2*

> *months. The term of the decision may be extended in accordance with the procedure for adoption of the decision…".*

Moreover, it is prescribed that the overall term of interception of correspondence and other communications, as well as wiretapping, cannot exceed 12 months.[48] We consider that rules on duration of interception in the AmLOIA are adequate, since they provide sufficient foreseeability regarding initial duration of the measure, conditions under which it can be prolonged and time after which it must be discontinued.

### 2.7.6 Procedures to be followed for storing, using, communicating and destroying the intercepted data

There are not many provisions in the AmCPC which regulate storing, using, communicating and destroying the intercepted data. Some of these rules are found in Article 241(5,6), which reads as follows:

> *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, which must literally reproduce the part of the conversation concerning the case. The record is attached to the protocol, and the irrelevant part of it is eliminated after the court verdict becomes res judicata or suspension of the case.*

In particular, we note that AmCPC does not require that data which are not relevant to the purpose for which they have been obtained be destroyed immediately. On the contrary, it is stipulated that "irrelevant part of it is eliminated after the court verdict becomes res judicata or suspension of the case". Armenian legislator might wish to rectify this shortcoming as soon as possible.

There are several, more detailed provisions in the AmLOIA. Firstly, as a rule, Article 8(3) of the AMLOIA mandates that all officers adhere to the principle of legality, in the following terms:

> *3. When carrying out their activity, officers of operational departments are guided by law and accountable to their immediate superior. When receiving an order or instruction, the officer of the operational department shall, in case of doubts regarding the lawfulness of the received order or instruction, immediately report in writing to the issuer of the order or instruction or the superior of the latter or their substitute. If the issuer of instruction confirms in writing the given order or instruction, the officer of the operational department shall execute it, unless the given order or instruction results in criminal liability prescribed by law. The person who has confirmed in writing the order or instruction.*

[48] AmLOIA, Article 39(2).

Next, Article 40(2) of the AmLOIA regulates the obligation to prepare record of operational intelligence measure:

> *2. The record of operational intelligence measures shall be drawn up by the official who conducts these measures. Records shall include the place, time, circumstances, name, family name, position of the officer carrying out operational intelligence measure and the names, family names, and positions of other participants of operational intelligence measure, as well as the names and family names of the persons (or their legal representatives) to whom the operational intelligence activities are applied in such a sequence as they have been carried out, scientific-technical methods and means used, as well as information, materials and documents acquired as a result of the measure. The record shall be signed by the official (officials) conducting operational intelligence measure.*
>
> *3. The rules for submitting the results of operational intelligence measures to bodies conducting criminal proceedings shall be prescribed by law and by legal acts of operational intelligence bodies. Operational intelligence body may communicate the information acquired during operational intelligence measures laid down in this Law only to bodies conducting criminal proceedings or to other operational intelligence bodies upon their request to exercise specific powers vested in them by law, except for the information that shall be destructed as prescribed by this Law.*

Finally, Article 6(1) contains some rules regarding the destruction of materials:

> *3. If a person, in cases and within the period referred to in part 1 of this Article, does not request materials and documents acquired as a result of operational intelligence measures carried out in his/her regard, these materials and documents shall be destructed.*
>
> *4. Materials referred to in part 2 of this Article shall be destructed within three months after the denial to institute a criminal case against him/her or termination of a criminal case against a person as a result of absence of incident of crime or corpus delicti in his/her conduct, or after the caused damage is deemed lawful under criminal law, or his/her acquittal.*

Here, we note that AmLOIA also does not require clearly that data which are not relevant to the purpose for which they have been obtained be destroyed immediately. This shortcoming should also be rectified in the future.

### 2.7.7 Notification of interception of communications and available remedies

Neither the AmCPC nor AmLOIA contain an obligation to notify the person concerned that his or her communications were intercepted.

AmCPC also does not prescribe whether the person who somehow knows or suspects that his or her communications have been intercepted has the right to request information about it. This shortcoming should be rectified, and appropriate notification procedure should be implemented in the AmCPC.

Unlike AmCPC, AmLOIA contains in its Article 6(1) at least a provision about publicity of materials and documents obtained as a result of operational-intelligence activity, which reads as follows:

> *1. Any person - within a period of three months after the denial to institute a criminal case or termination of a criminal case against him/her as a result of absence of incident of crime or corpus delicti in his/her conduct, or after the caused damage is deemed lawful under the criminal law, or his acquittal - shall be entitled to demand from bodies carrying out operational intelligence activity materials and documents acquired as a result of operational intelligence measures.*
>
> *2. Provision of these materials and documents shall be denied should it pose a threat of disclosure of state or official secret, or when the provision thereof may disclose secret staff officers of bodies carrying out operational intelligence activity and persons that have secretly cooperated or cooperate with these bodies.*

Finally, we note that Article 170(4) of the AmCPC provides that

> *Anyone who infringes on the inviolability of personal and family life shall be charged by law. Any harm caused to a person as a result of the disclosure of a personal or family secret shall be subjected to compensate the damages in the manner prescribed by law.*

### 2.7.8 Supervision

Finally, AmLOIA contains several provisions which seek to minimise risk of unauthorized use of interception measures.

To begin with, AmLOIA establishes a system of presidential oversight over the application of secret surveillance measures. Pursuant to its Article 31(4), "*The head of the Service shall submit to the President of the Republic of Armenia an annual report on each body authorised to carry out operational intelligence measures no later than January 31 of the next year which will contain the following information for the previous year: 1) total number of motions submitted to the Service for carrying out operational intelligence measures laid down in this Article; 2) number of motions brought without the extract of court decision, for which the extract was not submitted later; 3) number of motions brought without the extract of court decision, for which the court later denied authorisation to carry out such operational intelligence measures.*"

Next, AmLOIA also prescribes that official who has made a decision on conducting wiretapping directly monitors the execution of this measure, and holds personal liability for the lawfulness of its execution.[49] Additionally, operational-intelligence activities are also subject to monitoring by the prosecutor, who is responsible to ensure lawfulness of operational intelligence activity as well as confidentiality of the documents and information communicated by bodies carrying out operational intelligence activity.

[49] AmLOIA, Article 33.

# 3 Azerbaijan

## 3.1 Available statutes and other sources of information

This part of the Report is based on the following sources:

1. Code of Criminal Procedure of the Azerbaijan Republic (hereinafter: AzCPC)
2. Detective-Search Activity Act of the Azerbaijan Republic (hereinafter: AzDSAA)
3. Information provided by national stakeholders during the mission to Azerbaijan organized by the Council of Europe's Cybercrime Programme Office and held in Baku on October 12 and 13, 2017.

## 3.2 Expedited preservation of stored computer data

Azerbaijan did not implement expedited preservation of stored computer data (Article 16 of the Convention) as a standalone measure. In such circumstances, Azeri authorities apply Article 143(2) of the AzCPC to issue production order in circumstances when preservation of data is necessary.

Application of Article 143(2) does not give rise to issues regarding precision and foreseeability of national legislation. In essence, Article 143(2) provides for production of documents, and the notion of "document" includes, pursuant to Article 135(1)

> *"paper, electronic and other materials bearing information which may be of importance for the prosecution, in the form of letters, numbers, graphic of other signs…".*

Therefore, it is reasonably foreseeable that computer data can be subject to request stipulated in Article 143(2). However, the above-mentioned solution is not optimal in terms of proportionality. As explained in the introduction, full implementation of *all procedural powers* envisaged in the Section 2 of the Convention on Cybercrime, including preservation orders, enhances protection of fundamental human rights and freedoms *per se*. This is so because it enables the broadest application of the proportionality principle. Namely, if preservation would be implemented as a standalone measure, law enforcement authorities would have at their disposal less restrictive means to be used when the primary goal is only to secure the data. Therefore, in the context of AzCPC, we hold that introduction of standalone preservation orders would make it possible to use less intrusive procedural powers (where their use would be appropriate in given circumstances).

## 3.3 Expedited preservation and partial disclosure of traffic data

Situation with preservation of traffic data is similar as above (3.2). There is no specific provision covering preservation and partial disclosure of traffic data (Article 17 of the Convention) in the Azeri legislation. According to explanations given by national stakeholders, this is (looking from the perspective of law enforcement needs) partly compensated by the fact that communication services providers do retain some traffic data about their users' communication as a matter of business practice. Also, it was submitted that law enforcement

authorities have appropriate informal cooperation with the ISP's, which enables them to establish contact with relevant operator expeditiously and request preservation of certain data. Such requests are done in an informal manner and do not require any formal authorization; however, such authorization would be necessary to order production of the preserved information, or their seizure.

Notwithstanding the effectiveness of this system, we emphasize that any processing of personal data, which includes traffic data, interferes with Article 8 of the ECHR. As was elaborated in the introduction, such interference can be valid Article 15 and other international rules only if there is a proper legal basis for it, and if the relevant legal framework is sufficiently precise, foreseeable and contains adequate protection against arbitrary application. Consequently, we hold that, to achieve full compliance with requirements arising under Article 15 of the Convention, it is necessary to introduce precise and foreseeable legal basis for preservation and/or retention of traffic data.

## 3.4 Production order

As explained above, production of data can be requested on the basis of Article 143(2) of the AzCPC. Provisions of this article, read in conjunction with Article 135(1), are broad enough to encompass all types of computer data. Moreover, there is no dispute that, where available, subscriber information stored in any form could be subject to a request made on the basis of Article 143(2). On the other hand, there is no denying that provision stipulated in Article 143(2) does not differentiate between various categories of computer data.

## 3.5 Search and seizure of stored computer data

There are no specific provisions on search and seizure of stored computer data in the AzCPC. In such circumstances, legal rules for traditional search and seizure is applicable.[50] These rules are defined in Chapter XXX, articles 242 – 247 of the AzCPC. As a general rule, search can be executed "*where the available evidence or material discovered in a search operation gives 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*".[51] Moreover, "objects and documents which may be of significance as evidence may be impounded by the investigator". Once again, it is submitted that the notion of "document" includes computer data, pursuant to Article 135(1) which stipulates that document includes "*paper, electronic and other materials bearing information which may be of importance for the prosecution, in the form of letters, numbers, graphic of other signs…*". And although the notion of "document" is broad enough to include computer data, better solution would be to introduce more specific regulation, which would also take into account different categories of computer data.

Moreover, different options for seizing stored computer data, which are defined in Article 19(3) of the Convention, should be adequately reflected in national legislation. Currently, there is general agreement between the stakeholders that less intrusive methods of seizure (i.e., making and retaining a copy of stored computer data) can and in practice sometimes are used instead of more intrusive ones (seizing computer devices and/or storage mediums). Such interpretation is also supported by Article 245(3), according to which "the investigator shall be

[50] Chapter XXX of the AzCPC.
[51] AzCPC, Article 242(1).

entitled to conduct the search or seizure using photography, video, film or *other recording techniques*". But, this does not settle the issue completely, since in current legal regime national authorities have very broad margin of discretion when choosing among different modalities of conducting seizure. More appropriate approach would be the one where AzCPC would explicitly stipulate which are relevant options for executing seizure (in line with Article 19(3) of the Convention), and where would exist legal *obligation* on the part of investigators, prosecutors and the courts to use the least restrictive option.

In general terms, search and seizure rules contained in chapter XXX of the AzCPC provide for several safeguards.

Firstly, as a general rule, search and seizure is conducted on the basis of court warrant. Such warrant must be based on the basis of a reasoned motion from the investigator and submission made by the prosecutor.[52] In certain, highly limited circumstances, it is possible to conduct a search without the court order.[53] Nevertheless, it seems that rules regarding subsequent judicial control of a search conducted without court authorization are absent from the AzCPC.

Next, there are precise rules regulating the contents of a search warrant,[54] participation of circumstantial witnesses, defense counsel, interpreter, experts and other persons.[55]

Finally, AzCPC contains detailed rules governing the execution of search and seizure and recording of it.[56]

Other safeguards that should be addressed under domestic law include the right against self-incrimination, and legal privileges and specificity of individuals or places which are the object of the application of the measure.

## 3.6 Real-time collection of traffic data

Azeri legislation does not differentiate between real-time collection of traffic data (in line with Article 20 of the Convention) and interception of content data (Article 21). During the discussions, it was submitted that real-time monitoring of traffic data is not routinely done in practice; however, it was also explained that there were cases where real-time tracking of location data was done. In such circumstances, it is necessary to verify whether legislative framework for such actions is in place. According to one interpretation, both real-time collection of traffic data and interception of content data can in practice be executed on the basis of Article 259 of the AzCPC, which covers "*interception of conversations held by telephone and other devices, of information sent by communication media and other technical means, and of other information*". This solution is not completely satisfactory, for at least two reasons.

Firstly, Article 15 does not impose the same duties in relation to the real-time collection of traffic data and the interception of content data. In other words, conditions and safeguards associated with these measures do not necessarily have to be the same. Therefore, by

[52] AzCPC, Article 243(1).
[53] AzCPC, Article 243(3).
[54] AzCPC, Article 243(2).
[55] AzCPC, Article 244.
[56] AzCPC, Article 245-247.

implementing these measures independently of each other, Azeri authorities could better tailor their scope to their particular needs, while at the same time providing for greater flexibility and compliance with human rights requirements.

Secondly and more importantly, we are not convinced that Article 259 satisfies the requirements of legal precision and foreseeability, when it comes to real-time collection of traffic data. The main problem here is that text of this provision implies that its object is the *content of the communication*. This follows from the first paragraph of that article, which deals with "*interception of conversations … and of information sent by communication media and other technical means…*", and "*information sent or received by the suspect or the accused*". Also, the notion of "interception", as it is usually understood, refers to the content of the communication.[57] In such circumstances, it can be argued that citizens cannot foresee with reasonable certainty whether their traffic data can be collected in real-time on the basis of the AzCPC.

Similar situation is to be found in the AZDSAA. This act regulates, in its article 10, eighteen detective-search measures, among which are "tapping telephone conversations" and "retrieving of information from technical channels and other technical means". Unfortunately, none of these provisions is sufficiently precise and foreseeable to give indication whether it can be applied to real-time monitoring of traffic data.

## 3.7 Interception of content data

### 3.7.1 Legal basis

Interception of content data is, in the Azeri legislation, regulated by the AzCPC and the AzDSAA. Firstly, as noted above, Article 259 of the AzCPC regulates "*interception of conversations held by telephone and other devices, of information sent by communication media and other technical means, and of other information*". Moreover, its chapter XXXIII (Article 255 *et seq.*) also enables confiscation of "postal, telegraph and other messages". Finally, Article 10 of the AzDSAA stipulates that

> *I. Agents of the Detective-Search Activity shall be entitled to use the following detective-search measures in order provided by the present ACT:*
>
> *...*
>
> *3) tapping telephone conversations;*
>
> *4) examination of postal, telegraphic and other correspondence;*
>
> *5) retrieving of information from technical channels and other technical means;*

We consider that Article 259 of the AzCPC and some parts of Article 10 of the AzDSAA are sufficiently clear and foreseeable in defining their scope. On the other hand, we have some reservations regarding article 255 *et seq.* of the AzCPC, which enable confiscation of "postal, telegraph and other messages". The main issue here is that it is not clear what is meant by "other messages". Secondly, regarding Article 10(I) paragraphs 4 and 5 of the AzDSAA, while "tapping of telephone conversations", and "examination of postal and telegraphic

[57] Explanatory report to the Convention on Cybercrime, para 210.

correspondence" are sufficiently precise, it is not clear from the law what is meant by "examination of … other correspondence" and "retrieving of information from technical channels and other technical means". In this context, we note that AzDSAA does not define the scope of these procedural powers. As currently written, these provisions are overly vague and consequently do not give citizens adequate indication as to which means of communication can be subject to surveillance under law.

It is important to note here that application of the AzCPC and the AzDSAA is not necessarily linked. AzDSAA pursues wider range of aims, and does not contain any provision which would preclude application of detective-search measures independently of the AzCPC. In other words, it is possible to order interception in accordance with AzDSAA, without simultaneously applying AzCPC. This does not necessarily mean that Azeri legislation is inadequate; however, it is necessary to verify whether conditions and safeguards are adequately set in both statutes. On the contrary, different approach is used in other project countries, i.e. Moldova and Georgia. For instance, Moldovan law stipulates precisely that certain operative-investigative activities (including interception) can be performed only under the Criminal Procedure Code of the Republic of Moldova.[58] Similar solution can be found in Article 7(3) of the Georgian Law on Operative Investigatory Activities.[59]

## 3.7.2 The authorities' access to communications

Pursuant to Article 39 of the AzDSAA;

> *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.*

Therefore, it seems evident that Azeri legislation creates certain obligations for providers, who are required, *inter alia*, to implement "extra technical devices" in their networks, in order to enable execution of "search actions". While the exact scope of obligations under this provision is for obvious reasons classified and therefore not available to us, it seems reasonable to conclude that some possibilities of direct access to communications networks are present in the Azerbaijan. Since, as noted by the ECtHR and explained in the introduction, systems which enable direct access to communication infrastructure are "particularly prone to abuse", national legislation must ensure, with particular attention, that all appropriate safeguards against arbitrariness and abuse are adequately implemented. The effectiveness of those safeguards will be analysed below.

## 3.7.3 Authorization procedure

Regarding authorization procedure, Article 259 of the AzCPC stipulates that interception of communications "*shall as a rule be carried out on the basis of a court decision*". This is

[58] See chapter 6.7.1 below.
[59] See chapter 5.7.1 below.

confirmed by its Article 177(4), which mandates that certain investigative procedures can only be conducted on the basis of a court decision. Moreover, according to Article 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*".

By way of exception, investigator may

> "*intercept conversations held by telephone or other means and information sent via communication media and other technical means if there are circumstances in which evidence of serious or very serious offences against the individual or central government must be established without delay*".[60]

In such circumstances, the investigator is obliged to (a) inform, within 24 hours, the court exercising judicial supervision and the prosecutor in charge of the procedural aspects of the investigation of the investigative procedure conducted, and (b) submit the material relating to this investigative procedure, within 48 hours, 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.[61]

Similarly, pursuant to Article 10(4) of the AzDSAA, "*shall the grounds provided by the legislation of the Republic of Azerbaijan be present in the case, the Agents of the Detective-Search Activity are entitled, without due authorization of judge, as follows: 1) to tap telephone conversations; examine postal, telegraphic and other mail correspondence, retrieve information from technical channels and other technical means; as well as to shadow people for the purpose of preventing of grave crimes against individual or especially dangerous crime against the State*". In those circumstances, agents "*shall submit, within 48 hours, their substantiated decisions in written to the court that has the supervisory authority and the prosecutor in charge of procedural management of the pre-trial investigation*".

These procedures provide some safeguards against arbitrary application. Most importantly, subsequent judicial authorization is required. On the other hand, it would be beneficial if other safeguards were added in the law. Firstly, national law should stipulate that if subsequent judicial authorization is not received, or if the court considers that procedure was not conducted legally, interception must be terminated, and all collected information destroyed immediately. Moreover, we consider that deadline of 48 hours to present judicial approval might be too long. Consequently, Azeri legislator might wish to shorten this term, for instance to 24 hours.

Requirement to get a court warrant to conduct interception represents an important safeguard against arbitrary surveillance. However, the mere fact that interception needs to authorization the court is not sufficient, if the courts are not functionally empowered to analyse properly whether secret surveillance of communications is "necessary in a democratic society". According to the case-law of the ECtHR, this condition is satisfied if national courts are capable of verifying (a) "*the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures*", and (b) whether interception of content "*is proportionate to the*

[60] AzCPC, Article 177(4)4.
[61] AzCPC, Article 443(2)1-2.

*legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means*".[62] The purpose of this is to ensure that "*secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration*".[63]

Regarding the first of the above-mentioned conditions, it is stipulated in Article 259(1) of the AzCPC that it can be applied 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. Moreover, pursuant to Article 259(4)3, the decision authorising the interception must contain "*the objective grounds and reasons for intercepting the relevant conversations and information*". Therefore, the first condition seems to be satisfied. Regarding the second condition, there is no requirement in the AzCPC to show that the aims of criminal investigation and prosecution could not be achieved by some other, less restrictive means. This is a significant shortcoming in the law and should be addressed as soon as possible.

We turn now to the same conditions under the AzDSAA. Firstly, pursuant to its Article 13(I), measured discussed here

> *shall be allowed if there are sufficient grounds to believe that the measures carried out with a purpose of collecting information on the persons preparing for crime, attempting the commission of crime, committing crime, hiding themselves from court, investigation and inquiry bodies, evading punishment, as well as, of tracing stolen goods, of preventing concealment and destruction of evidence will produce information to serve as evidence in criminal proceedings…*

Moreover, Article 10(III) stipulate that

> *shall it be impossible to achieve the goals set in Section 1 of the present ACT; detective-search measures specified Para. 3-5, 8 and 10 of part I of this Section are to be exerted based on the decision of court (judge).*

Finally, Article 12(3) prescribes that decision in respect of operative-search measures relevant here must contain "*facts justifying the application of means and methods of intrusive nature*" and "*justification of non-possibility of obtaining the information through other methods*".

All of the above-mentioned conditions make it evident that provisions of the AzDSAA adequately implement the requirement of "necessity".

## 3.7.4 Scope of application

As explained in the introduction, international law requires that domestic legislation restricts the application of interception measures in relation to a limited range of serious criminal offences. Moreover, it requires also that national law defines with precision categories of people liable to have their communications intercepted.

Regarding the first of these requirements, we note with concern that neither the AzCPC nor the AzDSAA limit measures mentioned above to serious offences. The only mention of the gravity of offences in the context of surveillance can be found in Article 177(4)4 of the AzCPC

[62] Zakharov v Russia, ECtHR app. no. 47143/06, para 260.
[63] Zakharov v Russia, ECtHR app. no. 47143/06, para 257.

and Article 10(IV) of the AzDSAA, which stipulate that in cases of "serious or very serious offences against the individual or central government" urgent authorization procedures can apply.

Applying interception measure in relation to any criminal offence is not compatible with the principle of proportionality. This represents a serious shortcoming in the law and should be addressed as soon as possible.

Regarding the second condition (that national law defines precisely categories of people liable to have their communications intercepted), we note that the AzCPC limits interception order, pursuant to its Article 259, to the suspect or the accused.[64] This provision is sufficiently precise and foreseeable. On the other hand, pursuant to Article 11(IV) of the AzDSAA, "the decisions of courts (judges), investigation authorities or authorized Agents of Detective-Search Activity shall be accepted only in following cases:

> *1) within the framework of existing of criminal case;*
>
> *3) in case of obtaining reliable information, which is received from unbiased and known source, to the effect that a particular person is preparing, committing or have committed a crime even without the framework of the existing criminal case;*
>
> *4) in case of event infringing the national security and its defense capacity or prevention of this event;*
>
> *5) in case of a person concealing himself from court, investigation or inquiry, evading execution of punishment or missing person;*
>
> *6) in case of identification of unknown human body.*

Our concern here is that above-mentioned provisions are overly vague and overbroad. For instance, it is not clear from the law which events might infringe national security and its defense. Similarly, provisions such as "in case of obtaining reliable information, which is received from unbiased and known source, to the effect that a particular person is preparing, committing or have committed a crime" are overbroad, since they grant authorities applying them "an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse".[65]

## 3.7.5 The duration of interception

As explained in the introduction, according to the case-law of the ECtHR, there should exist "a clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled".[66]

Pursuant to Article 259(2) of the AzCPC, "*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*". In this context, it is also necessary to consider

[64] AzCPC, Article 259(1).
[65] Zakharov v Russia, para 248.
[66] Zakharov, para 250.

Article 259(4)(7), which stipulates that decision authorising the interception of conversations must contain "*the period for which interception of the conversations and information is to be carried out*". In this context, ordinary practice is that the authorizing authority (court) will stipulate duration of this measure. On the other hand, it is unexpected that AzCPC does not prescribe conditions under which interception could be prolonged.

Moreover, we note with regret that the AzDSAA does not contain provisions which would adequately limit the duration of detective-search measures. In this context, we recognize that Article 14(VI) of this statute stipulates only that "detective-search measures in progress shall be terminated in the following cases:

> *1. achievement of the goals provided by Section 1 of this ACT;*
>
> *2. lack of constituents of crime (mens rea and actus reus) in the action of the targeted person".*

Therefore, it follows that under the AzDSAA, detective-search measures can be applied for undefined time (that is, until the aim of the interception is achieved). The fact that AzDSAA does not contain adequate limitations of the duration of interception is a serious shortcoming in the law and should be rectified as soon as possible.

### 3.7.6 Procedures to be followed for storing, using, communicating and destroying the intercepted data

Next, national law should prescribe that any data which are not relevant to the purpose for which they have been obtained must be destroyed immediately.[67] This requirement is defined in a precise manner in Article 259(5) of the AzCPC ("Intercepted information not related to the case shall be immediately destroyed"). Similarly, Article 16(5) of the AzDSAA stipulates that "*information obtained as a result of the detective-search activity, which affect life, dignity and honor of a person but does not constitute an illegal action shall not be kept and must be destroyed.*"

To conclude, there are also several provisions in the AzDSAA which seek to minimise risk of unauthorized use of interception measures and material obtained in the course of such measures. Firstly, Article 19 of the AzDSAA provides that "*chiefs of the Agents of the Detective-Search Activity shall supervise of compliance with legislation in the course of organizing and implementing of the Detective-Search Activity and shall be held personally for defaults*". Next, Article 19(1) calls for judicial supervision of the detective-search activities, in accordance with the AzCPC. Thirdly, AzDSAA also provides for prosecutorial supervision in Article 20, which reads as follows:

> *I. Prosecutor-General of the Republic of Azerbaijan and the prosecutors commissioned by him/her shall carry out supervision of the compliance of the Agents of the Detective-Search Activity with the legislation.*
>
> *II. Chiefs of the Agents of the Detective shall be bound to submit documents related to reasons and grounds for carrying detective-search measures subject to the inquiries of the prosecutors in case of the latter receives materials, information and complaints of the citizens in respect of the violation of*

[67] Zakharov, para 253-256.

> *legislation in the course of implementation of the detective-search measures, as well as examines Lawfulness of rules and orders related to the implementation of the detective-search measures.*
>
> *III. Except for the cases of commission of crime, information on persons infiltrated into criminal groups and marginal associations, extra-personnel and secret employees shall be disclosed to the prosecutor with the written permission of these persons.*
>
> *IV. Information on the organization, tactics, methods and means of the detective-search activity shall be subject of the prosecutorial supervision.*
>
> *V. Prosecutor-General of the Republic of Azerbaijan and the prosecutors commissioned by him/her who supervise of the detective-search activity shall maintain confidentiality of information contained in the documents submitted to them.*

Finally, Article 21 of the AzDSAA establishes liability for breaching legislation during implementation of detective-search activity, in the following terms:

> *I. Organization and implementation of detective-search activity without due consideration to objectives, grounds and conditions provided by the present ACT, as well as, disclosure of information regarding this activity entrusted with them for official use shall be subject to criminal, administration and disciplinary liability subject to the legislation of the Republic of Azerbaijan.*
>
> *II. Shall the human rights and freedoms, interests of legal persons breached or the detective-search activity be carried out in respect of person not connected with violation of ACT, the Agents of the Detective-Search Activity are bound to restore violated rights and compensate for material and psychological damage.*

### 3.7.7 Notification of interception of communications and available remedies

Azeri law does not contain an obligation to notify the person concerned that his or her communications were intercepted. This is a serious shortcoming and should be addressed in the future.

### 3.7.8 Formalities

From the formal and procedural viewpoint, AzCPC stipulates in Article 259(4) that the decision authorising the interception of conversations must include "the name of the administration assigned the duty of intercepting the conversations or information". Moreover, it is prescribed that "*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*".

# 4 Belarus

## 4.1 Available statutes and other sources of information

## 4.2 General comment

Concerning the implementation of conditions and safeguards (Article 15 Budapest Convention), the national legislation recognizes some elements of limiting and controlling the procedures of more intrusive measures, such as search and seizure, real-time collection of traffic data and content interception. There is a room for implement more effective judicial authorization with regard to highly intrusive procedural powers. Regarding the judicial authorization, the system of safeguards and guarantees is not implemented in a way to support less intrusive procedural powers before more intrusive options are applied. There are no clear and enforceable regulations implementing Articles 16-18 Budapest Convention, that is reason why there is no coherent system of safeguards and guarantees which prevent and control the intrusion into the privacy of individuals.

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

Article 16 and 17 are not implemented as a standalone measure in the National law in Belarus, but there is a basis for interference in the national legislation. National legislation is published online and is accessible. Definitions of subscriber information and traffic data, are not implemented in national law as suggested by the Convention. An important note of this is a lack of distinction between subscriber and traffic data in respect to procedural powers that apply to all categories of data the possibility of a lighter procedures for access to subscriber information as opposed to traffic and content data should be in place.

The Decree of the President of the Republic of Belarus No. 60 "On the issues to improve making use of the national segment of Internet" (1 February 2010) was mentioned as a base for having procedures in place for Article 16 and 17, and also covers data retention and some of the issues which are subject-matter of Articles 16 and 17 Budapest Convention. The Decree also covers expedited preservation of stored computer data and expedited preservation and partial disclosure of traffic data. The preservation period in practice depends of the investigation, and Preservation period is not clearly stipulate in the law.

The Decree also mandates The national internet service providers put the measures in place in order to be able to identify users of their services and store their personal data, those measures are closely related with article 16 and 17 but cannot be consider that the Article 16 and 17 are full implemented as the retention of the data is not same with the scope of the Article 16 and 17.

## 4.4 Production order

Article 18 from the Budapest Convention can be recognized in Article 103, p. 2 of the Criminal Procedure Code of Belarus, but gives some general provisions on handover of documents and data by aby person on request of investigation or prosecutor. In addition, the Law on Agencies of Internal Affairs gives base to the internal agencies are authorized to perform an

investigation and collect information from different sources, when is necessary to seize documents and data and also to request and receive data and information from private sector and to inspect the suspicious activities.

The Article 18 is implemented in the Article 103, p. 2 of the Criminal Procedure Code of Belarus, but has not cover the full scope of the Article 18 from the Convention and there is not clear distinction in the legislation between production of subscriber information and other computer data.

Those measures cannot be considering as a full implementation of the scope of the Article 18 from the Budapest Convention.

Moreover, as noted previously, Article 18 of the Convention is implemented by provisions of *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, 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, …". The only safeguard mentioned in this part is obligation to compensate damage done during the execution of these measures.

## 4.5 Search and seizure of stored computer data

Article 19 Budapest Convention on the search and seizure of stored computer data can be generally recognized in the National legislation via traditional search provisions contained in chapter 24 of the Criminal Procedure Code. Also according the article 208 of the National CPC, searches 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 same way, Article 209 states that "reasonable evidence indicating that certain items or records which are critical for criminal investigations are available, provided that the location and possessor thereof have been clearly identified, constitutes grounds for a seizure". The national CPC of Belarus does not provide for judicial supervision of search and seizure measure, as the order of investigator or prosecutor and is sufficient in this respect the Article 210 of the Code of Criminal Procedure.

Implementation of special provisions in the context of search and seizure computer system and computer data provided by Article 19 (search of a connected system; making and retaining a copy of those computer data or computer data) is not recognized in the national CPC of Belarus. At the same time, provisions related to seizing or similarly securing computer data (p. 3(a)) and assistance of specialists in technical matters (p. 4) are covered by general regulations on seizures and involvement of specialists and experts in criminal proceedings.

## 4.6 Real-time collection of traffic data

Article 20 Budapest Convention, the real-time collection of traffic data in Belarus is performed on the basis of the National Law on Investigation Activities. The relevant provision in this regard is article 11, sub- paragraph 12, which provides for a power to "retrieve information

from telecom channels", as well as Article 18, sub-paragraph 12, which provides for a power to "exercise control in electronic communications networks".; no judicial authorization is provided.

Because the real-time collection of traffic data is considered to be the measure which limits constitutional right to privacy, Article 13 of the said Law stipulates that this measure under Article 12 can only be executed on the basis of prosecutor's warrant, upon a "well-grounded order of a respective agency responsible for operational investigation", while Article 19 of the said Law stipulates that measure under Article 18 can only be executed on the basis of a resolution issued by an authority conducting operational and search activities and sanctioned by the prosecutor or deputy thereof; no judicial authorization is provided in either case. Article 13 additionally provides for certain time-limits of the duration of the power to "retrieve information from telecom channels".

## 4.7 Interception of content data

Article 21 Budapest Convention the legal framework for interception of content data is recognized in several law provisions in National laws of Belarus. Article 214 of the National Code of Criminal Procedure provides a general power to monitor and record communications. According to this provision, "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 incharge investigator of the Investigative Committee, Chairman of the State Security Committee, or officials acting in their capacity"; no judicial authorization is provided. National legislation is stipulates the validity of the interception warrant, but not clear prescribe that any data which is not relevant to the purpose for which they been obtained must be destroyed. The national legislation gives some safeguards against the risk of unauthorized access to the intercepted data.

From the technical perspective, the interception of content data is facilitated by Decree of the President of Belarus of 3 March, 2010, No 129 "On Cooperation between Telecommunication Operators and Authorities conducting Operational and Search Activities".

# 5 Georgia

## 5.1 Available statutes and other sources of information

This part of the Report is based on the following sources:

1. Georgian Criminal Procedure Code (hereinafter: GeCPC),
2. Georgian Law on Operative Investigatory Activities (hereinafter: GeLOIA),
3. Georgian Law on Electronic Communications (hereinafter: GeLEC),
4. Information provided by national stakeholders during the mission to Georgia, organized by the Council of Europe's Cybercrime Programme Office and held in Tbilisi on October 19 and 20, 2017.

## 5.2 Expedited preservation of stored computer data

Georgian legislation does not recognize expedited preservation of stored computer data as a standalone measure. To achieve the purpose of Article 16 of the Convention, Georgian authorities rely upon Article 136 of the GeCPC, which regulates so-called "requesting a document or information" measure. As analysed below (5.2), provisions in Article 136 are sufficiently precise and foreseeable. Moreover, conditions and safeguard defined therein are sufficient to provide protection against arbitrary application of the law. However, we still hold that proper implementation of Convention's Article 16 would entail its introduction in the national legislation as a standalone measure. This is because full implementation of all procedural powers envisaged in the Section 2 of the Convention on Cybercrime, including preservation orders defined in Articles 16 and 17, in itself enhances protection of human rights and freedoms. Namely, if preservation orders are implemented as standalone measures in national legislation, law enforcement authorities have at their disposal less restrictive measure to be used when their primary goal is only to secure the data; otherwise, the only option is to secure it using production order, which is more intrusive compared to simply preserving data.

## 5.3 Expedited preservation and partial disclosure of traffic data

Next, expedited preservation and partial disclosure of traffic data (Article 17 of the Convention on Cybercrime) is also not present in the Georgian legislation as a standalone procedural power. In this context, we note that Georgia operates a complex data retention system, which is practice enables its authorities to achieve the purpose of Article 17 by other means (see below 5.6). Since data retention does not fall within the scope of the Convention on Cybercrime, it would be outside the scope of this report to analyse the compliance of Georgian legislation in the context of data retention with the fundamental rights and freedoms. Moreover, at the time of writing of this report, various legal issues pertaining to retention of traffic data and interception of content data have been subject to intensive public debate, legislative amendments as well as claims before the Constitutional Court of Georgia (see more extensively in chapter 5.6 below). In such circumstances, it is not possible to give adequate analysis of compliance with Article 15 requirements currently.

## 5.4 Production order

As explained above, measure corresponding to Article 18 of the Convention is found in Article 136 of the GeCPC, which regulates so-called "request for document or information" measure. Pursuant to the first paragraph of this article,

> *If there is a reasonable cause to believe that information or documents essential to the criminal case are stored in a computer system or on a computer data carrier, the prosecutor may file a motion with a court, according to the place of investigation, to issue a ruling requesting the provision of the relevant information or document.*

As is evident from the text of this provision, Article 136(1) applies to requests for "documents" or "information" stored in a computer system or on a computer data carrier. The first question here is whether the notions of "documents" and "information" include computer data. In this context, it was explained by national authorities that Article 136 needs to be interpreted in line with Article 3, para 23 of the GeCPC, according to which "*any source in which information is recorded in the form of words and signs and/or photo-,film-video-sound or other recordings, or through other technical means, shall be considered a document*". Since this definition is broad and yet foreseeable enough, we conclude that scope of Article 136(1) of the GeCPC is sufficiently precise and foreseeable and therefore acceptable from Article 15 perspective.

Moreover, second paragraph of Article 136 covers production of *"information about the user".* According to this provision,

> *2. If there exists reasonable cause to believe that a person is carrying out a criminal act through a computer system, the prosecutor may request a court, according to the place of investigation, to deliver a ruling ordering the service provider to provide information about the user.*
>
> *3. For the purposes of this article, information about the user shall be any information that a service provider stores as computer data or in any other form that is related to the users of its services, differs from the internet traffic and content data and which can be used to establish/determine:*
>
> *a) the type of communication services and technical means used, and the time of service;*
>
> *b) the identity of the user, mail or residential address, phone numbers and other contact details, information on accounts and taxes, which are available based on a service contract or agreement;*
>
> *c) any other information on the location of the installed communications equipment, which is available based on a service contract or agreement.*

It is obvious from the text of these provisions that they were drafted in accordance with Article 18(2-3) of the Convention on Cybercrime. In that context, it is important to note that the definition of "information about the user" for purposes of the GeCPC corresponds to the notion of subscriber information in the Convention on Cybercrime.

In order for Article 136 to be applied, there has to exist "*a reasonable cause to believe that information or documents essential to the criminal case are stored in a computer system or on a computer data carrier*". Moreover, Article 136 requires that the prosecutor files a motion with the court, and the production of document or information is granted only on the basis of a court order. Finally, Article 136(4) specifies that request for a document or information

prescribed by this Article is subject to the same procedures that apply to covert investigative actions under GeCPC, and Article 143[3] stipulates that a court ruling authorizing a covert investigative action or a prosecutor's decree on the conduction of such investigative action under urgency, as well as a subsequent court ruling finding the conducted covert investigative action lawful/unlawful shall be submitted to Personal Data Protection Inspector of Georgia without delay. All of these conditions constitute important safeguards against arbitrary application of the law.

In January 2017, Georgian Constitutional Court ruled in the case of *Nadia Khurtsidze and Dimitri Lomidze v. The Parliament of Georgi*a that paragraphs 1 and 4 of Article 136 are unconstitutional, to the extent that they prevent defence in criminal proceedings from obtaining computer data. In our opinion, this issue falls outside the scope of the Cybercrime Convention, since it concerns general principles of criminal proceedings. In such circumstances, we are of the opinion that the new CPC should address this issue by keeping existing conditions and safeguards which are necessary for the compliance with Article 15 of the Cybercrime Convention, and at the same time ensuring that concerns expressed in Constitutional Court's judgement are adequately addressed.

## 5.5 Search and seizure of stored computer data

Georgian CPC does not contain any specific rules applicable for computer-related search and seizure. In such circumstances, traditional procedural powers of search and seizure serve as a legal basis for search and seizure of computer data. Search and seizure is one of investigative actions, defined in the Chapter XV of the GeCPC, more specifically its Articles 119 and 120.

Pursuant to Article 119(1) of the GeCPC, this procedural power can be used to uncover and seize, inter alia, a "document" or "any other object" containing information which are essential to the case. This provision needs to be interpreted in conjunction with Article 3(23) of the GeCPC, which defines the notion of "document". As already explained above, this provision, read in conjunction with Article 3(23), is sufficiently precise and foreseeable.

In order to apply this procedural power, several conditions need to be satisfied.

Firstly, on-going formal investigation is an absolute prerequisite for search and seizure. Also, there should exist a probable cause, which is defined as "*a totality of facts or information that, [together] with the totality of circumstances of a criminal case in question would satisfy an objective person to conclude that a person has allegedly committed an offence; an evidential standard for carrying out investigative activities and/or for applying measures of restriction directly provided for by this Code*".

Secondly, pursuant to GeCPC, documents and/or information which are subject to search and seizure have to be essential to the case.

Thirdly, search and seizure are executed, as a general rule, on the basis of a court order. Only in cases of urgent necessity, search and seizure can be initiated on the basis of investigator's decree.[68] In such circumstances, it is necessary to follow procedure stipulated in Article 112, which reads as follows:

[68] GeCPC, Article 120(1).

*5. An investigative action stipulated by paragraph 1 of this article, in the case of urgent necessity, may also be carried out without a court ruling, when a delay may cause destruction of the factual data essential to the investigation, or when a delay makes it impossible to obtain the above data, or when an item, document, substance or any other object containing information that is essential to the case has been found during the conduct of any other investigative action (if found only after a superficial examination), or when an actual risk of death or injury exists; in that case, the prosecutor shall, within 24 hours after initiating the above investigative action, notify a judge under whose jurisdiction the investigative action has been carried out, or according to the place of investigation, and hand over the materials of a criminal case (or their copies), which justify the necessity of an urgent necessity in the conduct of the investigative action. Within not later than 24 hours after receipt of the materials, the judge shall decide the motion without an oral hearing. The judge may review a motion with the participation of the parties (provided that a criminal prosecution has been initiated) and the person against whom an investigative action has been carried out. When reviewing a motion, the judge shall check the lawfulness of the investigative action carried out without a court decision. To take explanations, the judge may to summon a person who carried out the investigative actions without a court ruling. In this case, when reviewing a motion, the procedure provided for by Article 206 of this Code shall apply.*

*6. After reviewing materials, the court shall deliver a ruling:*

*a) finding the conducted investigative action as lawful;*

*b) finding the conducted investigative action as unlawful and finding the information received as inadmissible evidence.*

*7. A court may hear a motion provided for by this article, without an oral hearing.*

*8. A court ruling delivered under this article shall be appealed in the manner provided for by Article 207 of this Code. The time limit for appealing a ruling shall commence from the day when the judgement is enforced.*

Moreover, several procedural safeguards are applicable within the framework of search and seizure. Thus, pursuant to Article 120(2) of the GeCPC, investigator is be obliged to present a court order, or in the case of urgent necessity, a decree, to a person subjected to the seizure or search. The presentation of the ruling (decree) must be confirmed by the signature of the person subject to search.

In our opinion, the main deficiency of search and seizure as it is currently regulated in the GeCPC is the lack of proper implementation of Article 19(3) of the Convention. According to explanations given by national stakeholders, in practice law enforcement authorities can and do use less intrusive methods of seizure (i.e., making and retaining a copy of stored computer data), instead of more intrusive ones (seizing computer equipment). Moreover, legislator's intent to enable the use of less-restrictive measures is visible also from Article 120(4), which stipulates that the "*investigator shall offer the person subject to the search, to voluntarily turn over an item, document, substance or any other object containing information that is subject to seizure. If an object that is subject to seizure is voluntarily provided, that fact shall be recorded in the relevant record. In the case of refusal to voluntarily turn over the requested*

*object, or in the case of its incomplete provision, it shall be seized by coercion*". But, although there seems to be no dispute whether current legal framework enables use of less intrusive methods of seizure, we believe that this should also be adequately reflected in the text of the GeCPC. Currently, it can be argued that law enforcement authorities and the courts have complete discretion over the method of conducting seizure. In our opinion, more adequate solution would be the one where investigators, prosecutors and the courts would be under a legal obligation to use the least restrictive tool.

In addition, more conditions and safeguards are provided for cases when it is necessary to execute a search at the 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[69] and 123[70].

## 5.6 Real-time collection of traffic data

There are several provisions which cover real-time collection of traffic data in Georgian legislation. Firstly, this issue is subject-matter of Article 137 of the GeCPC. But, at the same time, provisions of Georgian Law on Electronic Communications (GeLEC) are also applicable here. Since our first analysis in 2013, it was primarily the GeLEC which triggered most of the debate regarding conditions and safeguards applicable to surveillance of communications. The main question in this context concerned the powers of national authorities concerning direct access to the infrastructure of communication service providers and discrepancies between provisions of the GeCPC and GeLEC.

As a general rule, pursuant to Article $8^1$ of the GeLEC, electronic communication providers are obliged to enable real-time monitoring of their networks. Article $8^1$ reads as follows:

> *Upon the request of an authorised body, an electronic communications company should have a technical capability to deliver, in real time, to the monitoring system of an authorised body the content and identification data of communications sent via its networks.*

[69] **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.

[70] **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.

Therefore, GeLEC creates general conditions for surveillance of communications. It is important to note that technical capacity to monitor electronic communications includes both content data and traffic data. In the GeLEC, the term "identification data of communications" is used instead of "traffic data". Pursuant to Article 2($z^{69}$) of the GeLEC; it is defined as:

> *user identification data; data necessary for tracing and identifying a communication source; data necessary for identifying a communication addressee; data necessary for identifying communication date, time and duration; data necessary for identifying the type of a communication; data necessary for identifying user communication equipment or potential equipment; data necessary for identifying the location of a mobile communication equipment.*

Notion of "identification data of communications" includes also "user identification data" (presumably corresponding to subscriber information). Other than that, this notion includes the same categories of traffic data as the (now invalidated) EU Data Retention Directive. In our opinion, this provision is sufficiently precise and foreseeable.

More controversially, GeLEC contained in its Article $8^3$ more specific provisions dealing with covert investigative actions. Article $8^3$ read as follows:

> *Article $8^3$ - Conduct of covert investigative activities*
>
> *1. In order to carry out covert investigative activities, a duly authorised state body shall be entitled to:*
>
> *a) have a technical capability to obtain information in real time from physical lines of communication and their connectors, mail servers, base stations, base station equipment, communication networks and other communication connectors, and for this purpose, install, where necessary, a lawful interception management system and other appropriate equipment and software free of charge at said communication facilities. After obtaining information in real time, the authorised body shall implement measures independently on the basis of a court ruling or a reasoned resolution of a prosecutor;*
>
> *b) copy and store for two years the identification data existing in a communication channel. In that case, covert investigative actions after the removal and fixation of information from a communication channel/computer system shall be carried out by, the authorised body from the data banks of the said copied data on the basis of a court ruling or a reasoned resolution of a prosecutor.*
>
> *2. The architecture and appropriate interfaces of the technical capability for the real-time delivery of information shall be determined by an appropriate act of the State Security Service of Georgia.*

However, in April 2016 Constitutional Court of Georgia ruled that some parts of this article are incompatible with the Georgian Constitution, and requested that the parliament makes necessary changes by the end of March 2017. Legislative amendments were indeed enacted in due time, but they remain controversial, and are currently subject to another proceeding before the Constitutional Court. The final decision in this case is pending.

Moreover, legal basis for real-time collection of traffic data is found in Article 137 of the GeCPC, which reads as follows:

> *1. If there is reasonable cause to believe that a person is carrying out a criminal act through a computer system, the prosecutor may, according to the place of investigation, file a motion with a court for a ruling authorising a real-time collection of internet traffic data; under the ruling the service provider is obliged to collaborate with the investigation authorities and assist them, in real time, in the collection or recording of those internet traffic data that are related to specific communications performed in the territory of Georgia and transmitted through a computer system.*
>
> *2. A motion specified in paragraph 1 of this article shall take account of the technical capacities of the service provider to collect and record internet traffic data in real time. The period for collecting and recording internet traffic data in real time shall not be longer than the period required to obtain evidence for a criminal case.*

Looking from the perspective of the quality of law, these provisions are sufficiently precise and foreseeable. The notion of traffic data, which is used in Article 137, is defined in Article 3(30) of the GeCPC as

> *"any computer data related to communications and generated by a computer system that are part of a communications chain and that indicates the source of communication, destination, direction, time, date, size, duration and type of the basic service".*

Other safeguards also apply. Firstly, on-going investigation is a necessary condition to apply real-time monitoring of traffic. Also, this measure is executed only on the basis of a court warrant, which in itself represents an important safeguard against arbitrary application of the law.

Finally, Article 137(3) prescribes that "provisions of Articles $143^2$-$143^{10}$ shall apply to the investigative actions stipulated by this article". This essentially means that real-time collection of traffic data is subject to the same procedure and safeguards as other so-called secret investigative actions. These conditions and safeguards are analysed bellow (3.6).

In terms of oversight, GeLEC establishes in its Article $8^2$ general logging obligation, in the following terms:

> *An electronic communications company shall record instances when the identification data of electronic communications are transferred under Articles 112 and 136 of the Criminal Procedure Code of Georgia to relevant state bodies and shall provide the relevant information to the Personal Data Protection Inspector.*

Finally, collection of traffic data is possible also based on Law on Operative Investigatory Activities (GeLOIA). Pursuant to Article 7(h) of this statute, obtaining electronic communication identification data is defined as one of the operative-investigative activities. Pursuant to Article 7(3) of the GeLOIA, this measure can be applied in accordance with the procedure laid down in Chapter $XVI^1$ of the GeCPC, in the following cases:

> *when searching for a missing person; when searching for an accused or convicted person for the purpose of bringing him/her before a relevant state authority if such person avoids the application of coercive measures imposed on him/her or the serving of an imposed sentence; when searching for property lost as a result of a crime.*

It is important to note here that the definition of "electronic communication identification data", pursuant to Article 1(h) of the GeLOIA is the same as in the GeLEC. Moreover, we consider that the scope of this measure, as it is defined in the GeLOIA, is compatible with the principle of proportionality.

## 5.7 Interception of content data

### 5.7.1 Legal basis

Interception of content data is regulated in Article 138 of the GeCPC ("Obtaining content data"), which reads as follows:

> *1. If there exists reasonable cause to believe that a person is carrying out a criminal act through a computer system, the prosecutor may, according to the place of investigation, file a motion with a court for a ruling authorising the collection of content data in real time; under the ruling the service provider is obliged to collaborate with the investigation authorities and assist them, in real time, in the collection or recording of content data related to specific communications performed in the territory of Georgia and transmitted through a computer system.*
>
> *2. A motion specified in paragraph 1 of this article shall take account of the technical capacities of a service provider to collect and record content data in real time. The period for real-time collection and recording of content data shall not be longer than the period required to obtain evidence for a criminal case.*
>
> *3. Provisions of Articles $143^2$–$143^{10}$ shall apply to the investigative actions stipulated by this article.*

This provision is sufficiently precise and foreseeable. Moreover, we note that there is no corresponding power in the GeLOIA, which means that all procedural rules pertaining to interception are contained within one statute. This fact in itself enhances precision and foreseeability of the law.

Under the GeCPC, obtaining content data can be undertaken under conditions and safeguards which apply to secret investigative actions. These conditions and safeguards are defined in Articles $143^2$–$143^{10}$, which regulate secret investigative actions, and which relevant conditions and safeguards.

### 5.7.2 The authorities' access to communications

Georgia also operates a system which enables direct access to communication networks, for purposes of real-time collection of traffic data and interception of content data. There are several provisions which are relevant in this context.

Firstly, pursuant to Article $8^1$ of the Georgian Law on Electronic Communications (GeLEC), there exists an obligation for service providers to ensure "real time delivery of information related to communications sent via electronic communication networks". Pursuant to this article,

> *Upon the request of an authorised body, an electronic communications company should have a technical capability to deliver, in real time, to the monitoring system of an authorised body the content and identification data of communications sent via its networks.*

Moreover, we note that, pursuant to Article $8^3(1)$of the GeLEC, competent authority (State Security Service of Georgia) was entitled to

> *a) have a technical capability to obtain information in real time from physical lines of communication and their connectors, mail servers, base stations, base station equipment, communication networks and other communication connectors, and for this purpose, install, where necessary, a lawful interception management system and other appropriate equipment and software free of charge at said communication facilities.*

In this context, we recognize that the above-mentioned provision was declared unconstitutional by the decision No 1/1/625,640 of the Constitutional Court of 14 April 2016 (with its application deferred until 31 March 2017). Nevertheless, it is also our understanding that following legislative amendments in March 2017, relevant authorities maintain possibility of directly accessing communications networks (with some additional safeguards which were implemented in the law).

In the above-mentioned circumstances, we recall that, pursuant to the case-law of the ECtHR, systems which enable direct access to communication infrastructure are "particularly prone to abuse". Therefore, it is of fundamental importance that national legislation ensures that all necessary and appropriate safeguards against arbitrariness and abuse are implemented. The effectiveness of those safeguards will be analysed below. However, we note with satisfaction that a very important safeguard – mandatory logging of interception measures - is implemented in Article $8^2$ of the GeLEC. Namely, pursuant to this provision,

> *An electronic communications company shall record instances when the identification data of electronic communications are transferred under Articles 112 and 136 of the Criminal Procedure Code of Georgia to relevant state bodies and shall provide the relevant information to the Personal Data Protection Inspector.*

Substantially identical solution can also be found in Article $143^5$ of the GeCPC ("obligation of a body conducting secret investigative actions to store and keep record of information"). This provision reads as follows:

> *2. A body carrying out a secret investigative action shall keep a record of the following data related to the secret investigative action: the type of a secret*

> *investigative action; the start and end time of the secret investigative action; an object of a secret investigative action; if a secret investigative action under Article 143[1](1)(a-c) of this Code is carried out – a technical identifier of an object of a secret investigative action; the requisite details of a judge's ruling and/or of a reasoned resolution of a prosecutor.*

Finally, we note that the central database of electronic communication identification data, operated by Operative-Technical Agency (under State Secret Service of Georgia) falls under supervisory mandate of the Personal Data Protection Inspector of Georgia, in accordance with Article 351(4) of the Law on Personal Data Protection.

## 5.7.3 Authorization procedure

### 5.7.3.1 Authority competent to authorize interception

To begin, Article 143[3](1) stipulates that secret investigative actions shall be carried out under a court ruling. Competence for issuing such rulings is, as a rule, given to judges of district (city) courts. However, in cases where secret investigative actions must be taken against "a state political official, a judge and a person having immunity", they may to be authorized "under a ruling of a judge of the Supreme Court of Georgia, or upon a reasoned motion of the Chief or Deputy Chief Prosecutor of Georgia".[71]

Court ruling is made upon a prosecutor's reasoned motion. In its motion, prosecutor needs to refer to circumstances that confirm that (1) investigation or prosecution are conducted in relation to one of limited number of criminal offences (see below 5.7.3), (2) limitations regarding the categories of people have been satisfied (see below 5.7.3), and (3) necessity requirements are satisfied (see more extensively in this chapter).[72] In particular, investigator's motion must include "information on the investigative action (if any) that was carried out in accordance with this Code before the motion was filed and that did not allow for the achievement of the intended purpose."[73]

As an exception, it is also possible to order secret investigative action without judicial authorization (urgent authorization procedure), in accordance with to Article 143[3](6), which reads as follows:

> 5. *In the case of urgent necessity, when a delay may cause destruction of the facts significant to the case (investigation), or make it impossible to obtain those data, a secret investigative action may be carried out/commenced without a judge's ruling, under a reasoned resolution of a prosecutor. The resolution of a prosecutor must contain appropriate requisite details (date and place of drawing up the resolution; reference to the article of the Criminal Code of Georgia under which the investigation is in progress; the name and surname of a prosecutor, his/her signature; classification designation; seal), and an operative part of the resolution must contain the reference to an object/objects of the secret investigative action, as well as to the type of the secret investigative action carried out, and must set a period of time for the*

[71] GeCPC, Article 143[3](1, 17).
[72] GeCPC, Article 143[3](2).
[73] GeCPC, Article 143[3](3).

> *action to be carried out (specifying its start and end dates and time), which must not exceed 48 hours. If any of the secret investigative actions under Article 1431(1)(a-c) of this Code is carried out, an operative part of the resolution must also contain the reference to at least one appropriate detail of a technical identifier/identifiers of an object/objects of the secret investigative action. A prosecutor shall, not later than 24 hours from the time of commencing the secret investigative action specified in the resolution, file a motion with a district (city) court under the jurisdiction of which the secret investigative action was/is carried out, or with a court according to the place of investigation to recognise as lawful the secret investigative action carried out in the case of urgent necessity/in progress. In the motion, a prosecutor shall prove the existence of both circumstances stipulated in paragraph 2 of this article and of those that required an urgent conduct/commencement of the secret investigative action without a court ruling. A judge shall review a prosecutor's motion, in the manner prescribed by paragraph 5 of this article, within not later 24 hours after it has been submitted to the court. When reviewing a motion, the judge shall check whether the conducted/ongoing secret investigative action complies with the requirements of paragraph 2 of this article, also whether it was necessary to carry out the above action urgently, and shall issue a ruling on:*
>
> *a) recognition of the conducted secret investigative action as lawful;*
>
> *b) recognition of the ongoing secret investigative action as lawful and continuing a period of its conduct for not more than 48 hours. This period shall be counted from the time of commencing a secret investigative action specified in the resolution of a prosecutor;*
>
> *c) recognition of the conducted/ongoing secret investigative action as unlawful, its termination, annulment of its results and destruction of the material/information obtained as a result of the action.*

Moreover, we note that pursuant to the GeCPC, in cases of urgent authorization procedure prosecutor is also required to notify its resolution to the inspector of personal data protection, in a tangible (documentary) form.[74]

Another very important safeguard is contained in Article $143^3$(8), which stipulates that

> *8. If the prosecution considers it unnecessary to use the information obtained as a result of a secret investigative action conducted in the case of urgent necessity as evidence, the prosecution shall, not later than 24 hours after the secret investigative action is commenced, file a motion with the district (city) court under the jurisdiction of which the above action was carried out, or to the relevant court according to the place of investigation, and request a finding of that action as lawful. After a court delivers the relevant ruling, the information obtained as a result of secret investigative actions shall be immediately destroyed in the manner prescribed by Article $143^8$(5) of this Code.*

[74] GeCPC, Article $143^3$(6)

Finally, Article 143[6] of the GeCPC clearly stipulates the obligation to terminate interception if urgent authorization procedure is considered unlawful, or judicial authorization is not received:

> *4. If the court recognises as unlawful a secret investigative action commenced in the case of urgent necessity, or the 48-hour period specified in a resolution on conducting a secret investigative action commenced in the case of urgent necessity expires, a state body with an appropriate authority shall, upon receiving the court ruling, terminate the secret investigative action upon the expiry of the 48-hour period for conducting a secret investigative action commenced immediately or in the case of urgent necessity.*

Urgent authorization procedure, as regulated in the GeCPC, contains sufficient safeguards to protect against abuse of this procedural power. Consequently, we consider that these provisions are in line with in line with requirements arising under Article 15 of the Convention.

### 5.7.3.2 Authorizing authority's scope of review

Next, as explained in the introduction, interception of communications can only be used if the requirement of necessity in democratic society is satisfied. In this context, the ECtHR held that authorizing authority must be capable of verifying:

3) "the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures"

4) "whether the requested interception meets the requirement of "necessity in a democratic society", … including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means".[75]

GeCPC implements the first of these conditions by a provision which mandates that prosecutor's motion for carrying out secret investigative actions must refer to circumstances that confirm that

> *b) there is a reasonable cause to believe that a person against whom a secret investigative action is to be carried out, has committed any of the offences defined in sub-paragraph (a) of this paragraph (person directly related to the offence), or a person receives or transmits information that is intended for, or is provided by, a person directly related to the offence, or a person directly related to the offence uses the communication means of the person.*[76]

Regarding the second condition, a motion of the prosecutor must also refer to the circumstances that confirm that:

> *c) secret investigative actions are carried out due to urgent public necessity and are a necessary, adequate and proportional means for achieving legitimate goals in a democratic society, for ensuring national security or public safety,*

[75] Zakharov v. Russia, para 260 and other cases quoted there.
[76] Article 143[2](2)(b)

> *for preventing riots or crime, for protecting the interests of a country's economic welfare or any other person's rights and freedoms;*
>
> *d) as a result of the requested secret investigative action, the information essential to the investigation will be obtained and that information cannot be obtained through other means or obtaining it requires unreasonably great effort.*

Finally, pursuant to GeCPC, judge is required to provide justification for the existence of circumstances mentioned above (reasonable suspicion (para b), and necessity requirements, para c and d) in its ruling.[77] Identical requirements are applicable when urgent authorization procedure is followed. In such circumstances, we hold that Georgian legislation empowers authorizing authorities with adequate scope of review.

### 5.7.3.3 Precision of interception order's content

As explained in the introduction, ECtHR has held that interception authorisation "must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information".

This requirement is set in Article $143^3$(10) of the GeCPC, which stipulates that "an operative part of a judge's ruling must include:

> *…*
>
> *c) a resolution on recognising as lawful the conduct of a secret investigative action or the conducted/ongoing secret investigative action, which must precisely include what type of a secret investigative action is authorised or what action is recognised as lawful;*
>
> *…*
>
> *e) an object/objects of a secret investigating action;*
>
> *f) if any of the secret investigative actions under Article 1431(1)(a-c) of this Code is carried out – at least one appropriate detail of a technical identifier/identifiers of an object/objects of the secret investigative action that must be controlled within the scope of the secret investigative action;*
>
> *g) if necessary, the place of conducting a secret investigative action;*
>
> *…*

In the light of all the above-mentioned, we consider that Georgian legislation requires that content of interception order be adequately precise vis-à-vis persons whose communications are to be intercepted.

## 5.7.4 Scope of application

As explained in the introduction, international law requires that domestic legislation restricts the application of interception measures in relation to a limited range of serious criminal

[77] Article $143^2$(10)

offences. Moreover, it requires also that national law defines with precision categories of people liable to have their communications intercepted.

Georgian CPC addresses the first of these requirements in its Articles $143^2$(1) and $143^3$(2)(a). In essence, interception of content is limited to cases where an "*investigation has been initiated and/or criminal prosecution is conducted due to an intentionally serious and/or particularly serious offence"*, or several other, especially enumerated offences in the Georgian Criminal Code. This solution is in line with requirements arising under Article 15 of the Convention.

Secondly, regarding categories of people liable to have their communications intercepted, we note that Article $143^3$(b) of the GeCPC stipulates that a motion of the prosecutor requesting application of secret investigative action must refer to the circumstances that confirm that "*there is a reasonable cause to believe that a person against whom a secret investigative action is to be carried out, has committed any of the offences defined in sub-paragraph (a) of this paragraph (person directly related to the offence), or a person receives or transmits information that is intended for, or is provided by, a person directly related to the offence, or a person directly related to the offence uses the communication means of the person*". This provision is therefore compatible with Article 15 requirements.

Finally, we note that GeCPC contains a provision which requires "reducing the number of secret investigative actions to a minimum". Namely, pursuant to its Article $143^7$,

> *1. The body conducting secret investigative actions, also investigative authorities or persons, shall be obliged, within their powers, to limit, as much as possible, the monitoring of communications and persons that are not related to the investigation.*

Moreover, in the second and third paragraph of this Article, GeCPC introduces a safeguard protecting certain privileged communications.

> *2. Secret investigative actions against a clergy person, a defence counsel, a physician, a journalist and a person enjoying immunity may be carried out only where this is not related to obtaining information protected by law in the course of their religious or professional activities respectively.*
>
> *3. Information on a personal communication of a defence counsel obtained as a result of secret investigative actions shall be separated from the information on the communication conducted between the defence counsel and his/her client. The contents of the communication between the defence counsel and his/her client related to the defence counsel's professional activities shall be immediately destroyed.*

In the light of all the above-mentioned, we consider that Georgian legislation adequately limits the scope of application of interception measure.

### 5.7.5 The duration of interception

Next, Article 15(2) calls also for limitations of the duration of certain procedures, and the same requirement is expressed by the ECtHR. As stated in *Zakharov v Russia*, there should exist "*a clear indication in the domestic law of the period after which an interception warrant will*

*expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled*".[78]

Provisions corresponding to this requirement are found in Article $143^3$(12) of the GeCPC:

> *12. A ruling of a judge authorising the conduct of a secret investigative action shall be issued for a period that is required to achieve the goal of the investigation, but for not more than 1 month. If this period is insufficient, it may be extended for not longer than two months upon a reasoned motion of the prosecutor, under a court ruling, in the manner prescribed by this Chapter. A motion of the prosecutor shall include information on the data obtained as a result of the current secret investigative action and indicate the reasons due to which the data that would be sufficient for the investigation could not be obtained. A period for the conduct of a secret investigative action may be extended one more time, for no longer than three months, upon a motion of the Chief Prosecutor of Georgia. A period for the conduct of a secret investigative action may not be further extended.*

We consider that the above-mentioned provisions provide sufficient foreseeability as to the period after which an interception warrant will expire and the conditions under which a warrant can be renewed. Also, the maximum overall duration of interception is clearly defined in law. Moreover, we note that Article $143^6$ creates additional grounds for termination of secret investigative actions. Pursuant to these provision, interception can be terminated even before the expiry of the term for which it was authorized, if:

> *a) a specific objective stipulated by a ruling on a secret investigative action has been accomplished;*
>
> *b) circumstances are discovered that confirm that the specific objective stipulated by the ruling on the given secret investigative action cannot be achieved due to objective reasons, or the conduct of the secret investigative action id no longer essential to the investigation;*
>
> *c) the investigation and/or criminal prosecution is terminated;*
>
> *d) there is no more legal ground for carrying out a secret investigative action.*
>
> *3. If the period for carrying out a secret investigative action expires, or the grounds for suspending a secret investigative action is not removed within three days after it was suspended, a state body with an appropriate authority shall terminate the secret investigative action upon the expiry of the period specified in this paragraph.*

Finally, we note that GeCPC contains one solution which is unique in the legislation of the project countries, and that is the institute of "suspension of a secret investigative action". Namely, pursuant to Article Article $143^6$(5) of the GeCPC, secret investigative action may be suspended by the inspector of personal data protection through an electronic control system if:

> *a) an electronic copy of the judge's ruling on granting permission to carry out a secret investigative action under Article $143^1$(1)(a) of this Code, which contains*

[78] Zakharov v Russia, para 250.

> *only the requisite details and an operative part, has not been forwarded to him/her under the procedure established by Article 143[3](5[1]) of this Code;*
>
> *b) a copy of the ruling on granting permission to carry out a secret investigative action under Article 143[1](1)(a) of this Code, which contains only the requisite details and an operative part, has not been forwarded to him/her under the procedure established by Article 143[3](5) of this Code, in a tangible (documentary) form;*
>
> *c) an electronic copy of a prosecutor's resolution, which contains only the requisite details and an operative part, has not been forwarded to him/her under the procedure established by Article 143[3](6[2]) of this Code;*
>
> *d) a copy of a prosecutor's resolution on conducting a secret investigative action under Article 143[1](1)(a) of this Code in the case of urgent necessity, which contains only the requisite details and an operative part, has not been forwarded to him/her under the procedure established by Article 143[3](6[2]) of this Code, in a tangible (documentary) form;*
>
> *e) the requisite details and/or an operative part of the prosecutor's resolution submitted to him/her through an electronic system or in a tangible (documentary) form contain an ambiguity or irregularity;*
>
> *f) any data under Article 143[3](6) of this Code in the requisite details and an operative part of an electronic copy of a prosecutor's resolution submitted to him/her through an electronic system, and in the requisite details and an operative part of a prosecutor's resolution submitted to him/her in a tangible (documentary) form fail to coincide with each other.*

In cases of suspension of secret investigative actions, additional conditions and safeguards apply (see Articles 143[6](6-13). Most importantly, pursuant to Article 1436(16), "if the grounds for suspending a secret investigative action are not removed within three days after it was suspended, the material obtained as a result of the secret investigative action shall be destroyed under the procedure established by this Code".

In our opinion, conditions and safeguards mentioned above are sufficient to ensure protection against abuse of the law.

### 5.7.6 Procedures to be followed for storing, using, communicating and destroying the intercepted data

In this part, we begin by noting that GeCPC obliges bodies conducting secret investigative actions to store and keep records of information. Namely, pursuant to its Article 143[5],

> *1. A body carrying out secret investigative actions and relevant investigative authorities shall be responsible for appropriately safeguarding the information obtained as a result of secret investigative actions.*
>
> *2. A body carrying out a secret investigative action shall keep a record of the following data related to the secret investigative action: the type of a secret investigative action; the start and end time of the secret investigative action; an object of a secret investigative action; if a secret investigative action under Article 1431(1)(a-c) of this Code is carried out – a technical identifier of an*

> *object of a secret investigative action; the requisite details of a judge's ruling and/or of a reasoned resolution of a prosecutor.*

Next, Article $143^6$(14) contains an obligation to create a protocol about every secret investigative action:

14. A state body with an appropriate authority shall draw up a protocol upon completion of a secret investigative action. The protocol shall exactly specify the legal grounds for conducting the secret investigative action, its start and end time, the place where the protocol was drawn up, the type of the conducted secret investigative action and the technical means used for its conduct, a place of conducting a secret investigative action, an object of a secret investigative action, and if any of the secret investigative actions under Article $143^1$(1)(a-c) of this Code is conducted – also a technical identifier of an object of a secret investigative action. This protocol shall be forwarded to an appropriate authorised investigative body which will immediately submit it to the prosecutor, the court register of the secret investigative actions and to the inspector of personal data protection. The protocol shall also be forwarded to the defence in the cases provided for in, and under the procedure established by this Chapter.

Moreover, "When a secret investigative action is carried out, if requested by a prosecutor/judge, a body conducting the secret investigative action shall issue an interim protocol".[79]

Next, we note that GeCPC contains in its Article $143^9$(1) a provision which mandates that

> *only investigators, prosecutors and judges may, before the completion of secret investigative actions, examine the information obtained as a result of those actions (provided that such information is substantially related to the issue that they are to review).*

Finally, we recognize that GeCPC contains detailed rules on destruction of information and materials obtained as a result of secret investigative actions. This is regulated by Article $143^8$, which reads as follows:

> *1. Information obtained as a result of secret investigative actions shall, by decision of the prosecutor, be immediately destroyed after the termination or completion of such actions, unless the information is of any value to the investigation. Also, the information obtained as a result of the secret investigative action that has been carried out without a ruling of a judge in the case of urgent necessity and that, even though recognised by a court as lawful, has not been submitted as evidence by the prosecution in the manner prescribed by Article 83 to the court that hears the case on the merits. The materials shall be immediately destroyed if they are obtained as a result of operative-investigative activities and do not concern a person's criminal activities but include details of that person's or any other person's private life and are subject to destruction under Article 6(4) of the Law of Georgia on Operative-Investigative Activities.*
>
> *2. Materials obtained as a result of secret investigative actions, which are recognised by a court as inadmissible evidence, shall be immediately destroyed six months after the court of the final instance renders a ruling on the case.*

[79] Article $143^6$(15)

*Until destruction, these materials shall be kept in a special depository of a court. No one may access these materials, or make copies of them or use them, except for the parties who use them for the purpose of exercising their procedural powers.*

*3. The materials obtained as a result of secret investigative actions that are attached to a case as the material evidence shall, under Article 79(2) of this Code, be kept in the court for the period of keeping this criminal case. After the expiration of this period, the above materials shall be immediately destroyed.*

*4. In cases provided for by paragraphs 2 and 3 of this article, an administration of the court that kept the material before its destruction shall be responsible for adequate keeping of the material obtained as a result of secret investigative actions.*

*5. In the cases provided for in paragraph 1 of this article, the information obtained as a result of secret investigative actions shall be destroyed by a prosecutor providing procedural supervision over the investigation of the given case, or supporting the state prosecution or by their superior prosecutor, in the presence of a judge or of a judge of the court who or whose judge made a decision on the conduct of this secret investigative action, or recognised as lawful or unlawful the secret investigative action carried out without a court ruling in the case of urgent necessity. A record of the destruction of materials obtained as a result of secret investigative actions, signed by the relevant prosecutors and judges, shall be handed over to the personal data protection inspector, and shall be included in the court registry of secret investigative actions.*

*6. In cases provided for by paragraphs 2 and 3 of this article, the materials obtained as a result of secret investigative actions shall be destroyed by the judge or by a judge of that court who, or the judge of which, made a decision on the conduct of the secret investigative action or recognised as lawful or unlawful the secret investigative action that was carried out without a curt ruling in the case of urgent necessity.*

Finally, we note that Personal Data Protection Inspector, as part of its supervisory mandate over law-enforcement authorities, monitors whether the competent authorities adhere to the obligation of destruction/deletion of information obtained as a result of secret investigative actions. In our opinion, conditions and safeguards mentioned above, viewed as a whole, are sufficient to ensure reasonable protection against possible abuses of the law.

### 5.7.7 Notification of interception of communications and available remedies

As noted in the introduction, the ECtHR holds that notification of interception of communications "is inextricably linked to the effectiveness of remedies before the courts". In this context, we note that GeCPC contains several provisions dealing with notification requirements and procedures.

Pursuant to Article 143[9],

> *(3) A person against whom a secret investigative action has been carried out, shall be notified in writing of the conduct of that action as well as of the contents of the materials obtained as a result of that action and of the destruction of the above material. Along with that information, such person shall also be presented with a court ruling on the conduct of secret investigative actions against him/her, as well as the materials based on which the judge rendered such a decision, and shall be informed of the right to appeal the above ruling in the manner prescribed by Article 143[3](15) of this Code. A decision as to the time when a person is to be notified of the conduct of secret investigative actions against him/her and be handed over the relevant ruling and materials, shall be made by the prosecutor, both during and after the legal proceedings, taking into account the interest of the legal proceedings.*
>
> *4. If a prosecutor decides not to notify a person of the conduct of secret investigative actions against him/her within 12 months after the conduct of the secret investigative actions, the prosecutor shall be obliged, within not later than 72 hours before the expiration of the above term, to file a motion with the court whose judge rendered the ruling on the conduct of the secret investigative actions, and request the postponement, for no longer than 12 months, of the provision of information to the relevant person on the conduct of the secret investigative actions. The motion shall provide reasons why the notification of the person could pose a risk to the achievement of the legitimate goal of the investigative actions, to the accomplishment of the objectives and to the interests of legal proceedings. A judge shall review the motion, in the manner prescribed by Article 112 of this Code, within 48 hours after it has been filed, at his/her own discretion, with or without oral hearing. When reviewing a motion with an oral hearing, the judge shall ensure the participation of the relevant prosecutor in the review with a relevant notification. His/her non-appearance shall not impede the review of the motion. After the review, the judge shall make a decision to grant the prosecutor's motion and to postpone the notification of the relevant person or to reject the motion and refuse to postpone the provision of such information to the relevant person. A prosecutor shall, not later than 72 hours before the term for notifying the person of the conduct of a secret investigative action expires, be obliged to apply to a court with a motion stipulated by this paragraph and request the extension of this term for not longer than 12 months.*

Also, it is stipulated in paragraph 2 of this article that "the information obtained as a result of secret investigative actions shall be provided to the party according to Article 83(6), also in the case of approval of a plea bargain".

In our opinion, notification procedure under the GeCPC is consistent with the ECtHR's requirement that "as soon as notification can be carried out without jeopardizing the purpose of the restriction after the termination of the surveillance measure, information should … be provided to the persons concerned". In this context, we are glad to note that Georgian legislator decided to implement a system of mandatory notification, which is not dependant on any specific request made by the concerned person.

### 5.7.8 Supervision

Finally, we note that the GeCPC, as amended in the period after the previous report (2013), now contains additional requirements also in the context of overall supervision over application of interception measures. In this context, Article 143[10], which regulates so-called registry of secret investigative actions, provides as follows:

> *1. The Supreme Court of Georgia shall prepare a registry of secret investigative actions, which shall include statistical information on secret investigative actions, in particular: information on motions filed with the courts for the conduct of secret investigative actions, and on ruling rendered by courts on those motions, as well as information on the destruction of materials obtained as a result of operative-investigative actions that did not concern criminal activities of the given person but which, include details on that or another person's private life and that has been destroyed in accordance with Article 6(4) of the Law of Georgia on Operative-Investigative Activities.*
>
> *2. The Supreme Court of Georgia shall, at the end of every year, publish the information provided for by paragraph 1 of this article.*

Finally, we note that Personal Data Protection Inspector submits annual report to the Parliament on the state of personal data protection in the country. A separate chapter of the report contains results of monitoring of investigative activities under Articles 136-138 and covert investigative activities under Article 1431(1)(a-b) of the GeCPC respectively.

# 6 Moldova

## 6.1 Available statutes and other sources of information

This part of the Report is based on the following sources:

1. Moldovan Code on Criminal Procedure (hereinafter: MdCPC),
2. Moldovan Law on preventing and combating cybercrime (hereinafter: MdLPCC),
3. Moldovan Law on Special Investigative Activity (hereinafter: MdLSIA),
4. Moldovan Electronic Communications Act (hereinafter: MdECA),
5. Information provided by national stakeholders during the mission to Moldova organized by the Council of Europe's Cybercrime Programme Office and held in Chisinau on November 2 and 3, 2017.

## 6.2 Expedited preservation of stored computer data

Expedited preservation of stored computer data (Article 16 of the Convention) is covered, at least in part, by the Moldovan Law on preventing and combating cybercrime (MdLPCC). Pursuant to Article 4(4)(a) of this law, Office of the Prosecutor General has competence to coordinate

> *"during the prosecution process, at the request of criminal prosecution body or official, the immediate preservation of computer data or of traffic data, which are in danger of destruction or alteration, under criminal procedure legislation".*

In cases where the holder of computer data is a service provider, Moldovan authorities rely on Article 7(1) of the MdLPCC, which stipulates that service providers are obliged:

> *"c) to perform, confidentially, the competent authority's request regarding the immediate preservation of computer data or of traffic data, which are in danger of destruction or alteration, within 120 calendar days, under the provisions of national legislation", and*
>
> *g) ensure the decipherment of the computer data contained in the network protocol packets with the preservation of these data for a period of 90 calendar days.*

In this context, it should be noted that the notion of "computer data" is defined in Article 2 of the MdLPCC, as

> *"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".*

Moreover, "traffic data" and "service provider" are also defined in the same article, which reads in relevant parts:

> *"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",*
>
> *"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"*

MdLPCC's definition of "computer data" is compatible with the same notion in Section 1(b) of the Convention, and the notion of "traffic data" is identical to the one used in Convention's Article 1(d). Therefore, we conclude that Article 7 of the MdLPCC satisfies the requirement of legal precision and foreseeability.

Next, we note that Article 7(1)(c) of the MdLPCC calls for a preservation period of 120 days. Admittedly, this period is longer than the one envisaged under the Convention. However, since preservation orders interfere only minimally with the interests of data holders, and since the Convention allows its parties to renew preservation orders and thus prolong the duration of their application, we do not consider this discrepancy to be a serious problem under Article 15. Nevertheless, Moldovan legislator might consider harmonizing preservation period completely with Article 16 of the Convention.

Article 7(c) of the MdLPCC is applicable only to data held by service providers. On the other hand, the scope of Convention's Article 16 is broader, since it is applicable to data held by any natural or legal person. Therefore, MdLPCC does not cover the whole subject-matter of Article 16. According to explanations provided by national authorities, it is possible to order natural and legal persons other than service providers to preserve computer data in their possession by applying general powers given to the prosecutors. Unfortunately, we were not provided with the text of those provisions, so we could not verify their compliance with Article 15 requirements. Nevertheless, based on our understanding of the applicable legal framework as elaborated by the national stakeholders, we don't see any issues arising under Article 15 here.

## 6.3 Expedited preservation and partial disclosure of traffic data

As explained above, Article 7 of the MdLPCC enables specifically preservation of traffic data (in addition to preservation of computer data in general). Firstly, pursuant to Article 7(1)(c) of the MdLPCC, service providers have the duty

> *c) to perform, confidentially, the competent authority's request regarding the immediate preservation of computer data or of traffic data, which are in danger of destruction or alteration, within 120 calendar days, under the provisions of national legislation.*

This provision satisfies Moldova's obligation under Article 17(1)(a) of the Convention. Moreover, it is important to note that Article 17(1)(b) of the Convention is reflected in Article 7(2) of the MdLPCC, which stipulates that

> *If the 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.*

As elaborated above, notions of "traffic data" and "service provider" are sufficiently precise and foreseeable. But, there are several other provisions of the MdLPCC, which add some ambiguity here. Namely, pursuant to its Article 7, service providers are also obliged to

> *f) to ensure the monitoring, supervision and storage of traffic data for a period of 180 calendar days, in order to identify service providers, service users and the channel by means of which the communication has been transmitted*

Article 7(f) of the MdLPCC seems to introduce a retention obligation ("storage of traffic data") for a period of 180 days. But, at the same time, general data retention obligation is prescribed in Article 20(3)(c) of the MdECA, which stipulates that providers of electronic communications networks and/or services shall be obliged:

> *c) to keep all available, generated or processed information in the process of providing its own electronic communications services necessary for identifying and tracking the electronic communications source, identifying the destination, type, date, time and duration of the communication, identifying the user's communication equipment or to another device used for communication, identification of the coordinates of the mobile terminal equipment, and to ensure that this information is presented to the bodies empowered under the law. Information on mobile or fixed telephony services will be kept for a period of one year, and those related to the Internet network of 6 months upon expiry of which the said information will be irreversibly destroyed by automated procedures, except for information and documents processed in accordance with art. 62[4] and those which, according to the normative acts in force, are kept for a longer period. The retention obligation also includes unsuccessful attempts to call.*

At this point, we note that there is some discrepancy between MdLPCC, which calls for storage of traffic data for a period of 180 days, and MdECA, which differentiates between telephone traffic data and internet traffic data. In our opinion, preservation obligation should be completely separated from provisions which deal with data retention. Moreover, having two laws which provide for essentially the same obligations, but with different modalities, is not compatible with the requirements of precision and foreseeability. Consequently, we propose that provisions of MdECA and MdLPCC, in part where they relate to retention obligation, be harmonized. Ideally, it would be beneficial to regulate retention obligation only in one of these statutes.

## 6.4 Production order

Article 18 of the Convention is only partially implemented in the MdLPCC. Namely, Article 7(a, d) of the MdLPCC obliges service providers:

> *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;*

The notion of "data about user" or "user data" is defined in Article 2 of the same statute, which reads as follows:

> *user data - any information in the form of computer data or in any other form held by a service provider relating to the subscribers of these services, other than traffic or content data, and which allow the determination of: the type of service the communications used, the technical provisions taken in this respect and the period of service; identity, postal or geographical address, subscriber's telephone number and any other contact number, as well as billing and payment data available under a contract or service arrangement; any other information concerning the location of the communication equipment available under a contract or service arrangement as well as any other data that may lead to the identification of the user.*

Legal basis for requesting production of user data is found in Article $134^5$ of the MdCPC, which covers "Identification of a Subscriber, Owner or User of the Electronic Communication System or of the Access Point to an Information System" and reads as follows:

> *(1) Identification of a subscriber, owner or user of an electronic communication system or of an access point to an information system implies requesting an electronic service provider to identify the subscriber, owner or user of the telecommunication system, of the telecommunication means or of an access point to an information system, or to communicate whether a particular means of communication or access point to an information system is used or is active or was used or was active at a certain date.*
>
> *(2) Besides the elements provided under article 255, the order to carry out the special investigative measure shall also include the following information:*
>
> *1) identification data of the service provider who holds the data specified in para. (1) or keeps them under control;*
>
> *2) identification data of the subscriber, owner or user, if known; motivation of meeting the conditions for ordering the special investigative measure;*
>
> *3) record about the obligation of the person or service provider to communicate immediately the information requested, based on confidentiality criteria.*
>
> *(3) Service providers must cooperate with the criminal investigative bodies in order to ensure enforcement of the prosecutor's order and provide them immediately with the requested information.*
>
> *(4) Persons called to cooperate with the criminal investigative bodies must observe confidentiality of the carried out operation. Violation of this obligation shall be punished under the Criminal Code.*

Unlike some other special investigative actions (i.e., interception of content), which can be authorized only under the MdCPC, production of subscriber information can also be ordered on the basis of Article 28 of the MdLSIA, which contains provisions substantially identical to Article $134^5$(1, 2) of the MdCPC. Pursuant to Article $132^2$(2)(a) of the MdCPC, identification of the subscriber, the owner or user of an electronic communication system or of an access point to an information system can be authorized by a prosecutor (unlike more intrusive measures, which require judicial authorization). Identical solution is found in Article 20(2) of the MdLSIA.

We consider that the above-mentioned rules covering production of "user data" are sufficiently precise and foreseeable, and otherwise in compliance with requirements arising under Article 15 of the Convention on Cybercrime. On the other hand, we note that Moldovan legislation does not implement more general part of Convention's Article 18, namely the one which calls for production of computer data in general, by any natural and legal persons. In such circumstances, it is necessary to use search and seizure measure, which is not adequate solution from the perspective of the proportionality principle. Consequently, we propose that this issue be considered by Moldovan authorities, and that relevant legislation be amended in order to ensure full compliance with Article 18.

## 6.5 Search and seizure of stored computer data

In the Moldovan CPC, there are no rules which are tailored specifically for search and seizure of stored computer data, in line with Article 19 of the Convention. Therefore, Moldovan authorities apply traditional powers of search and seizure of objects and documents to computer data as well. This is done in accordance with the Chapter III (Sources of evidence and evidentiary methods), Section 4 (Search for and Seizure of Objects and Documents) of the MdCPC.

From the perspective of Article 15, the first question here is whether the scope of search and seizure in accordance with Section 4 of the MdCPC is sufficiently precise and foreseeable. Pursuant to Article 125(1) of the MdCPC, it is possible to conduct search and seizure of "objects" and "documents". Similarly, Article 126 of the MdCPC stipulates that "*criminal investigative body shall have the right to seize any objects or documents …*". These provisions need to be interpreted in line with Article 157(1) of the MdCPC, which prescribes that

> *"material sources of evidence are documents in any form (written, audio, video, electronic, etc.) originating from officials or legal entities if they describe or confirm circumstances important for the case".*

Consequently, it seems reasonable foreseeable that the notion of document includes computer data.

As a general rule, search can be conducted when

> *"the evidence obtained or the operative investigative materials substantiate a reasonable assumption that the tools designed to be used or used as the means for committing a crime, objects and valuables obtained as a result of a crime are at a specific premises or in any other place or with a specific person".*

In the alternative, search can also be initiated

> *"for objects or documents that could be important for the criminal case and that cannot be obtained by other evidentiary methods".*[80]

In procedural terms, search must be based on a reasoned order of the criminal investigative body and the authorization of the investigative judge.[81] The same is also true for seizure.[82] Only in the case of "flagrant crime", a search may be based on a reasoned order without the

[80] MdCPC, Article 125(1).
[81] MdCPC, Article 125(3)
[82] MdCPC, Article 126(3)

authorization of a judge. In those circumstances, investigative body has the duty to submit to the investigative judge (within 24 hours) the materials obtained as a result of the search and transcript indicating the reasons for the search.[83] The investigative judge then verifies the legality of search done without previous judicial order, confirms its results if the search was legal or declares it illegal otherwise.[84]

Article 19/3 of the Convention specifies that 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.

Unfortunately, these provisions are still not implemented in the MdCPC. To be sure, there is no obstacle in the MdCPC to apply options stipulated in Article 19(3) of the Convention in practice. This was explicitly confirmed by different stakeholders during the meetings for the preparation of this study. But, although there seems to be no dispute whether current legal framework enables use of less intrusive methods of seizure, we believe that this should also be adequately reflected in the text of the MdCPC. Currently, it can be argued that law enforcement authorities and the courts have complete discretion over the method of conducting seizure. In our opinion, more adequate solution would be the one relevant authorities would be under a legal obligation to use the least restrictive tool.

In addition to the conditions described above, MdCPC incorporates several additional procedural conditions and safeguards. These include the following:

- There are rules stipulating that certain persons must be present during search. This includes person against whom the measure is applied, or members of his/her family, or other person who represents his/her interests; representative of enterprises or organizations whose premises are being searched)[85];
- It is forbidden to conduct a search during night time (128/1),
- 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).
- According to article 126/3, seizing of objects and documents can be done on the basis of explained and motivated warrant, issued by the criminal prosecution body. For these rules to apply, it is necessary that accumulated evidence or information from 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 authorization (126/2).

[83] MdCPC, Article 125(4)
[84] MdCPC, Article 125(4, 5)
[85] MdCPC, article 127.

## 6.6 Real-time collection of traffic data

Legal basis for real-time collection of traffic data in Moldovan legislation is Article 134[4] of the MdCPC, which covers so-called "collection of information from electronic communication service providers". Article 134[4] reads as follows:

> *Collecting information from electronic communication service providers and computerized data traffic implies collecting from telecommunication institutions, from wired or mobile phone operators and internet operators of information sent by technical telecommunication channels (telegraph, fax, paging, computer, radio and other channels), of confidential recording of information transmitted or received through technical lines of telecommunication links by the persons subject to special investigative measure and receiving from the operators of information about the users of telecommunication services, including roaming, and about telecommunication services provided to them, which include:*
>
> *1) holders of phone numbers;*
>
> *2) telephone numbers registered on the name of a person;*
>
> *3) telecommunication services provided to the user;*
>
> *4) communication source (the caller's phone number; first and last name, address of the subscriber or registered user);*
>
> *5) communication destination (telephone number of the appellant or the number to which the call was routed, redirected; first and last name, domicile of the subscriber or the respective user);*
>
> *6) type, date, time and duration of the communication, including failed call attempts;*
>
> *7) user's communications equipment or another device used for communication (IMEI of the mobile phone, Cell ID location name);*
>
> *8) location of the mobile communication equipment at the beginning of communication, geographical location of the cell.*

Identical provision is mentioned in Article 18(1)(h) of the MdLSIA. However, we note that Moldovan legislation stipulates that measure in question can only be performed[86] and authorized[87] under the Criminal Procedure Code of the Republic of Moldova" (while some other such actions can be done both in a criminal process, as well as outside it). Therefore, MdCPC will contain all relevant conditions and safeguards.

Collection of information from electronic communication service providers (Article 134[4]) is one of the so-called special investigative activities in the MdCPC. As such, a series of conditions and safeguards limit its application. Most importantly, this measure requires judicial authorization, can be applied only for a limited catalogue of criminal offences, under the further condition that it is necessary; moreover, its duration is limited in time. These and other conditions are elaborated upon below (7.7).

[86] MdLSIA, Article 18(3).
[87] MdLSIA, Article 20(1).

In general, conditions and safeguards applicable to this measure are compatible with Article 15. The main issue here is some ambiguity regarding the subject-matter of Article $134^4$. Namely, from the text of this provision it is not sufficiently clear what is meant by "information sent by technical telecommunication channels" and "confidential recording of information transmitted or received through technical lines of telecommunication links". Our concern here is that phrases quoted above might be interpreted as including some content data (see also below, 4.7). On the other hand, the non-exhaustive list of information about telecommunication services provided to users adds significantly to the precision and foreseeability of this provision. To conclude, Moldovan legislator might want to clarify the scope of these provisions, and to draw a clear distinction between collection of traffic data and interception of content data. Other than that, Article $134^4$ is compatible with requirements arising under Article 15 of the Convention on Cybercrime.

## 6.7 Interception of content data

### 6.7.1 Legal basis

Legal basis for interception of communication content data is found in Section 5 of the MdCPC and Article 18 of the MdLSIA. Under both statutes, interception falls under the scope of so-called special investigative activities.

In the context of the MdCPC, these activities are listed in Article $132^2$(1)(1) and include, *inter alia*, "wiretapping and recording of communications or images",[88] "apprehension, investigation, delivery, search or seizure of postal correspondence",[89] "monitoring the connections of telegraph and electronic communications"[90] and "collection of information from electronic communication service providers"[91].

Article 18(1) of the MdLSIA contains similar list of special investigative measures. It is important to understand that MdLSIA differentiates among three categories of special investigative actions: (1) those which are performed with the authorization of the investigating judge, at the request of the prosecutor, (2) those which are performed with the authorization of the prosecutor, and (3) those which are performed with the authorization of the head of the specialized subdivision of the competent authority. Only the first of these categories contains measures which correspond to Article 21 of the Convention on Cybercrime. Pursuant to Article 18(1)(1), it includes

> *c) the interception and recording of communications and images;*
> *d) retention, research, deliver, searches or seizure of postal items;*
> *e) monitoring the telegraph and electronic communication connections;*
> *h) collection of the information by the electronic communication service providers;*

It is obvious that the list of relevant special investigative actions in MdLSIA corresponds to the one in Article $132^2$(1)(1) of the MdCPC.

[88] MdCPC, Article Article 132(1)(1)(c)
[89] MdCPC, Article Article 132(1)(1)(d)
[90] MdCPC, Article Article 132(1)(1)(e)
[91] MdCPC, Article Article 132(1)(1)(h)

We note with satisfaction that Moldovan legislation stipulates precisely that above-mentioned special investigative actions are performed[92] and authorized[93] only in a criminal process under the Criminal Procedure Code of the Republic of Moldova" (while some other such actions can be done both in a criminal process, as well as outside it).

What is the scope of these measures? Pursuant to Article $132^8$(1) of the MdCPC,

> *"wiretapping and recording of communications imply the use of technical means ensuring finding out the contents of the conversations held between two or more persons and their recording implies storing on a technical media of the information obtained following the wiretapping".*

It follows from this provision, as well as other articles of the MdCPC (e.g., Article $132^9$, which mentions "listening" and "viewing" of conversations) that its object are voice and video conversations.

Regarding "apprehension, investigation, delivery, search or seizure of postal correspondence", the wording and overall scheme of corresponding Article 133 implies that its object is correspondence in tangible form. This follows also from Article 134, which stipulates that the measure is to be executed in post offices. However, second paragraph of Article 133 stipulates that *e-mail communications* can also be subject to it. It therefore seems obvious that this measure also corresponds, at least in part, to Article 21 of the Convention on Cybercrime.

Moreover, "monitoring the connections of telegraphic and electronic communications, includes, pursuant to Article $134^1$,

> *"the access and verification, without notifying the sender or the recipient, of the communications that were sent to the institutions providing electronic mail delivery or other communication services and incoming and outgoing calls of the subscriber".*

Finally, "collection of information from electronic communication service providers" implies, inter alia, collecting

> *"of confidential recording of information transmitted or received through technical lines of telecommunication links by the persons subject to special investigative measure".*

In this context, we note that subject-matter of above-mentioned measures is not sufficiently clear. For instance, it is not easy to understand what is the relation between Articles 133 and $134^1$, when the object of surveillance is e-mail correspondence. Similarly, it remains vague whether proper legal basis for surveillance of voice communications is Article $132^8$ (wiretapping) or Article $134^1$ (where it relates to incoming and outgoing calls of the subscriber). This vagueness is not such to bring into question the overall foreseeability of the law, since it is obvious that all methods of communication can be intercepted on the basis of MdCPC, but it would nevertheless be beneficial be address this issue in the future, and clarify the subject-matter of the relevant provisions. In this context, we believe that introducing specific provision which would create legal basis for interception of all computer data which are transmitted as content of some communication would provide necessary precision.

[92] MdLSIA, Article 18(3).
[93] MdLSIA, Article 20(1).

Speaking about requirements under Article 15 of the Convention on Cybercrime, namely conditions and safeguards necessary to ensure adequate protection of fundamental rights and freedoms, we note that open criminal investigation is the basic requirement for the execution of measures described above. Moreover, since these measures fall within the scope of special investigative activities, there are several conditions and safeguards which are applicable equally to all of them.

## 6.7.2 Authorization procedure

### 6.7.2.1 Authority competent to authorize interception

Regarding authorization procedure, both the MdCPC and the MdLSIA require court warrant. Pursuant to Article $132^2(1)(1)$ of the MdCPC, all the above-mentioned measures require authorization of the investigative judge. In this context, they differ from other special investigative measures, which can be executed with authorization of the prosecutor. Further, MdLSIA follows the same principle, which is evident from its Article 18(1).

In exceptional circumstances, a reasoned order of the prosecutor may be sufficient to authorize special investigative actions. This can happen

> *"in flagrant cases, and when there are circumstances that do not allow delay and when the court order cannot be obtained without the risk of an essential delay which may lead to the loss of evidence or immediately endanger the security of persons.*[94]

In such circumstances, it is necessary to inform the investigative judge within 24 hours about measures undertaken by prosecutor's order. Also, all materials justifying the need to carry out special investigative measures without court's authorization must be submitted to the investigative judge, who shall decide, by reasoned ruling, on the lawfulness of such measure.[95] Moldovan urgent authorization procedure contains most important safeguards against abuse. Moreover, we believe that law should stipulate that if judicial authorization is not received, or if the judge considers the measure to be unlawful, interception must be terminated, and all information and materials destroyed immediately.

### 6.7.2.2 Authorizing authority's scope of review

Next, we look at the authorization authority's scope of review. As explained in the introduction, the ECtHR has held that this authority it must be capable of verifying (1) the existence of a reasonable suspicion against the person concerned, and (2) whether the requested interception meets the requirement of "necessity in a democratic society", which implies that the aim pursued by law enforcement authorities cannot be achieved by less restrictive means. The purpose of this is to ensure that "*secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration*".[96]

[94] MdCPC, Article $132^4(3)$.
[95] MdCPC, Article $132^4(3)$.
[96] Zakharov v Russia, ECtHR app. no. 47143/06, para 257.

In this context, Article 132[1](2) of the MdCPC is relevant. This article stipulates that special investigative measures can be ordered and executed only if all the following conditions are met:

> *1) achieving the goal of the criminal proceeding is otherwise impossible and/or administration of evidence can be considerably damaged;*
>
> *2) there is reasonable suspicion that a serious, especially serious or exceptionally serious crime is prepared or committed, with the exceptions provided by the law;*
>
> *3) the action is necessary and proportionate restriction of the fundamental human rights and freedoms.*

On the normative level, these provisions are adequate from the perspective of Article 15 requirements. Moreover, the issue of establishing necessity for surveillance measures was discussed with national authorities, who submitted (although they were not able to produce any statistical data during the timeframe of writing this report) that following ECtHR's judgement in *Iordachi and Others v. Moldova*, Moldovan legislator and the courts are taking significant steps to ensure proper balancing of all interests involved, when deciding about surveillance warrants.

### 6.7.3 Scope of application

As explained in the introduction, international law requires that domestic legislation restricts the application of interception measures in relation to a limited range of serious criminal offences. Moreover, it requires also that national law defines with precision categories of people liable to have their communications intercepted.

In Moldovan law, this requirement is implemented in Article 132[1] of the MdCPC, which stipulates that special investigative actions can be ordered in cases related to serious, especially serious and exceptionally serious crimes. Moreover, it is important to note that in cases of wiretapping, more restrictive list of criminal offences applies. Namely, pursuant to Article 132[8]:

> *(2) Provisions of para. (1) shall apply exclusively to the criminal cases the object of which is the criminal investigation or trial of persons in whose regard there are data or evidence that he/she committed the crimes set forth in the following articles of the Criminal Code: arts.135–145, 150, 151, 158, 164-165[1] . art.166 paras.(2) and (3), art. 166[1] , 167, art.171 paras.(2) and (3), art. 172 paras. (2) and (3), arts. 175, 175[1], art.186 paras.(3)-(5), art.187 paras.(3)-(5), art.188, 189, art.190 paras.(3)–(5), art.191 para.(2) letter d) and paras. (3)-(5), art. 192[1] para. (3), art. 201[1] para. (3), arts. 206, 207, 208[1], 208[2], art.216 para.(3), art. 217 para. (3), art.217[1] paras. (3) and (4), art. 217[3] para. (3), art.217[4] paras. (2) and (3), art. 219 para. (2), art. 220 paras. (2) and (3), art. 224 paras. (3) and (4), arts. 236, 237, art. 241[1] para. (2), arts. 242[1]-243, art. 244 para. (2), art. 248 paras. (2)-(5), arts. 259-261[1], 275, 278-279[1], art. 279[2] para. (3) letter b), art. 280, 282-286, 289-289[3], art. 290 para. (2), arts. 292, 295-295[2], art. 303 para. (3), arts. 306-309, 318, 324-328, 333-335, art. 335[1] para. (2), arts. 337-340, 342-344, art. 352 para. (3), arts. 362,*

> *362[1], art. 368 para. (2), art. 370 paras. (2) and (3). The list of the component elements of the crime is exhaustive and may be amended only by law.*

Secondly, international law also requires that national law defines with precision categories of people liable to have their communications intercepted. In this context, we note that Article 132[8] of the MdCPC specifies that

> *(3) Subject to wiretapping and recording may be the communications of the suspect, accused or other persons, including the persons whose identity was not established, in whose regard there are data reasonably leading to the conclusion that they either contribute, in any manner, to the preparation, commission, favoring or hiding of the crimes listed in para. (2), or receive or transmit information relevant and important for the criminal case.*
>
> *(4) Subject to wiretapping and recording may be the communications of the victim, injured party, his/her relatives and family members, as well as of the witness, provided there is an imminent danger to his/her life, health or other fundamental rights, if it is necessary to prevent the crime, or provided there is an obvious risk to irremediably lose or distort the evidence. The wiretapping and recording of communications within the meaning of this paragraph shall be ordered according to the procedure set forth in art. 132[4] and only upon written consent or preliminary written request of the persons specified in this paragraph. The measure ordered according to this paragraph shall be terminated immediately after disappearance of the ground on which the authorization was based or upon express request of the person in whose regard the measure was ordered.*

Similarly, regarding "apprehension, investigation, delivery, search or seizure of postal correspondence", it is stipulated in Article 133(1) that this measure is applicable to mail correspondence received or sent by the suspect or the accused. Consequently, we consider that provisions mentioned above are sufficiently precise and foreseeable. On the other hand, we are not able to reach the same conclusion regarding the action of "monitoring the connections of telegraph and electronic communications". The main problem here is that Article 134[1] of the MdCPC does not contain any limitations regarding categories of people whose communication can be subject to it. Moldovan legislator might wish to address this issue in future amendments of the MdCPC.

Finally, certain communications are exempted from wiretapping. Pursuant to Article 132[4](10) of the MdCPC, this includes "relations of legal assistance between the lawyer and his/her client".

### 6.7.4 The duration of interception

Next, Article 15(2) calls also for limitations of the duration of certain procedures, and the same requirement is expressed by the ECtHR. As stated in *Zakharov v Russia*, there should exist "*a clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled*".[97]

[97] Zakharov v Russia, para 250.

In Moldovan CPC, it is stipulated that

> "special investigative measure shall be ordered for 30 days with the possibility of reasonable extension for up to 6 months, with exceptions provided by this Code. Each prolongation of the special investigative measure may not exceed 30 days. If authorization of the special investigative measure was extended for up to 6 months, repeated authorization of the special investigative measure based on the same grounds and on the same subject shall be prohibited, except for the use of undercover agents or occurrence of new circumstances, examination of the facts related to the investigation of organized crime and financing of terrorism, as well as searching for the accused".[98]

Moreover, MdCPC prescribes that

> *"if during examination of the report it is established that the conditions of prolongation of the special investigative measure are not observed or the rights and legitimate interests of individuals are disproportionally or manifestly violated by the ordered measure, or the grounds for the interference have disappeared, the prosecutor or the investigative judge shall order termination of the measure".*[99]

Finally, it is the duty of the prosecutor to order termination of special investigative measure

> *"as soon as the grounds and reasons justifying its authorization have disappeared, without the right to order resumption of the measure".*[100]

Such decision can also be made upon motion of the criminal investigative officer or the investigative officer, who have obligation to give such proposal to the prosecutor, if they believe that he grounds for carrying out special investigative measures no longer exist.[101] Under these circumstances, we consider that Moldovan law if sufficiently precise and foreseeable, and that it gives adequate notice about the duration of interception warrants, their possible renewal and termination.

**Illegality of evidence**

$132^5$(5) Should the prosecutor or the investigative judge establish that the measure was carried out with obvious violation of human rights and freedoms or the investigative officer exceeded the provisions of the order/authorization ruling, the prosecutor or the investigative judge shall declare the transcript null and void and shall order by an order/ruling immediate destruction of the material carrier of information and of the materials collected during the special investigative measure.

(6) Should the prosecutor or the investigative judge establish that the investigative officer's actions obviously violated the human rights and freedoms, the prosecutor or the investigative judge shall declare the carried out measures null and notify the competent authorities thereof. The prosecutor's order may be appealed to a higher-level prosecutor. The ruling of the investigative judge shall be irrevocable. When examining the legality of carrying out the

[98] MdCPC, Article $132^4$(7).
[99] MdCPP, Article $132^4$(6).
[100] MdCPP, Article $132^4$(8).
[101] MdCPP, Article $132^4$(9).

special investigative measure, the prosecutor or the investigative judge shall review the manner of carrying out the measure, the observance of the conditions and grounds which served as the basis for ordering the special investigative measure.

### 6.7.5 Procedures to be followed for storing, using, communicating and destroying the intercepted data

In relation to "Wiretapping and Recording of Communications", most of these procedures is regulated by Article $132^9$ of the MdCPC. In this context, we recognize that the following important safeguards are applied:

- Wiretapping and recording of communications are carried out by the criminal investigative body or the investigative officer. "Employees of the subdivision within the institution authorized by law, who shall technically ensure the wiretapping and recording of communications, as well as the persons who directly listen to the recordings, the criminal investigative officers and the prosecutor must keep the communications confidential and be liable for violation of this obligation".[102]
- "The technical subdivision of the body authorized by law to conduct wiretapping and recording of communications shall send online to the criminal investigative body the signal of wiretapped communications and other information indicated in the excerpt from the ruling of the investigative judge without their recording".[103]
- "The information collected in the course of wiretapping and recording of communications may be listened to and viewed online by the criminal investigative body and the prosecutor".[104]
- The information collected in the course of wiretapping and recording of communications shall be transmitted by the technical subdivision that carried out wiretapping to the criminal investigative officer or the prosecutor on a material information carrier, which shall be packed and sealed with the stamp of the technical subdivision along with indication of the sequence number of the information carrier. [105]
- There are special rules regarding the transcript of wiretapping and recording of communications. It must include: the date, place and hour when the transcript were prepared, the position of the person who carried out the special investigative measure, the number of the criminal case file in which the special measure was carried out, a record about the order of the prosecutor and the ruling of the investigative judge authorizing the special measure, the identity data and technical identification data of the subject whose communications were wiretapped and recorded, the period of time within which wiretapping of communications was carried out, a record about the use of technical means, other relevant information received following the wiretapping and recording of communications related to the identification and/or location of some subjects, the quantity and identification number of material information carriers on which the information was recorded, the number of verbatim transcribed

[102] MdCPC, Article $132^9$(1).
[103] MdCPC, Article $132^9$(4).
[104] MdCPC, Article $132^9$(5).
[105] MdCPC, Article $132^9$(6).

communications. A verbatim record of the communications important for the criminal case shall be attached to the transcript.[106]

- The wiretapped and recorded communications shall be integrally stored on the initial carrier submitted to the criminal investigative body by the technical subdivision. The investigative judge who authorized the special investigative measure shall keep the carrier.[107]
- Within 48 hours after the deadline for authorization of wiretapping and recording has expired, the prosecutor shall submit to the investigative judge the transcript and the original carrier of the recorded communications. The investigative judge shall issue a ruling on the observance of the legal requirements in the course of wiretapping and recording of communications by the criminal investigative body, shall decide which of the recorded communications shall be destroyed and shall designate persons responsible for destruction. Destruction of information based on the ruling of the investigative judge shall be recorded by the responsible person in the transcript attached to the criminal case file.[108]

### 6.7.6 Notification of interception of communications and available remedies

Moldovan law contains an important safeguard in Article $132^7$(7,8), which provides for notification to person who was subjected to special investigative measure. Relevant provisions of this article read as follows:

> *(7) If legality of the special investigative measure is established by an order/ruling, the prosecutor or the investigative judge who authorized the measure shall inform the persons who were subjected to the special investigative measure. During the criminal investigation, the investigative judge or the prosecutor may postpone, by a reasoned judgment, the notification of the person subjected to the special investigative measure, however, not later than upon termination of the criminal investigation.*
>
> *(8) As of the moment of notification set forth in para. (7), the person subject to the special investigative measure shall be entitled to take knowledge of the transcript on the special investigative measure and the material carrier of information, as well as of the order of the prosecutor or the ruling of the investigative judge on the legality of the carried out measure.*

[106] MdCPC, Article $132^9$(8).
[107] MdCPC, Article $132^9$(13).
[108] MdCPC, Article $132^9$(15).

# 7 Ukraine

## 7.1 Available statutes and other sources of information

This part of the Report is based on the following sources:

1. Ukrainian Code on Criminal Procedure (hereinafter: UaCPC),
2. Information provided by national stakeholders during the mission to Ukraine, organized by the Council of Europe's Cybercrime Programme Office and held in Kyiv on November 13 and 14, 2017.

## 7.2 Expedited preservation of stored computer data

Ukrainian law does not recognize expedited preservation of stored computer data (Article 16 of the Convention) as a standalone measure. According to explanations provided by national stakeholders, Ukrainian authorities achieve the purpose of this provision by securing the possession of data. This is usually done on the basis of Article 159 of the UaCPC, which regulates so-called "provisional access to objects and documents" (see below 7.4).

As we noted above, while analysing laws of other project countries, the use of traditional powers of production or seizure might be efficient enough and can therefore satisfy the needs of law enforcement authorities. But, this does not necessarily mean that such solution is completely satisfactory from the perspective of protection of fundamental human rights and freedoms. As explained in the introduction, the main issue in this context is the application of the proportionality principle. In short, we hold that *full implementation of all procedural powers* envisaged in the Section 2 of the Convention on Cybercrime enhances *per se* level of protection of fundamental human rights and freedoms. This is so because it enables the use of less intrusive procedural powers, instead of more intrusive ones.

We also note here that the issue of preservation and production of traffic data is highly contentious in Ukrainian law and policy. During the discussions with national stakeholders, it representatives of private sector objected repeatedly to the application of more intrusive powers, such as those under Article 159 of the UaCPC, where less intrusive methods (such as data preservation) would be sufficient. We believe that these problems are a direct consequence of shortcomings in legislation, namely, non-existence of less intrusive powers. We also note that relevant opinions in this matter have already been expressed by Council of Europe's experts,[109] and that proposals for legislative amendments have also been given.[110]

In this context, it bears noting once again that Article 15(3) of the Convention requires that its parties consider the "*impact of the powers and procedures … upon the rights, responsibilities and legitimate interests of third parties*" ("*to the extent that it is consistent with the public interest, in particular the sound administration of justice*"). Since the application of more intrusive powers, and in particular seizure of computer data and devices, interferes significantly with the interests of business operators, we believe that it is necessary to undertake additional steps to ensure that relevant legal framework enables full application of the proportionality principle, by introducing standalone preservation orders. Moreover, since

[109] See Report on Ukraine on Current legislation and draft laws supplementing and amending various issues related to cybercrime and electronic evidence, November 2016.
[110] See Expert Opinion on Draft amendments to the legislation of Ukraine concerning cybercrime and electronic evidence, May 2017.

Article 15 requires not only that adequate legal framework is set in written law, but also that it is applied in a proportionate manner, it is necessary to undertake additional steps to ensure that, whenever it is possible and acceptable from the perspective of efficiency of criminal proceedings, the least restrictive measures are used in practice.

## 7.3 Expedited preservation and partial disclosure of traffic data

Regarding Article 17 (expedited preservation and partial disclosure of traffic data), it first needs to be noted that there is no differentiation in the UaCPC between different types of computer data (i.e., subscriber information, traffic data and content data). Also, UaCPC does not contain any provisions designed specifically for expedited preservation and partial disclosure of traffic data.

On the other hand, it is important to note that there is a general data retention obligation for telecommunication service providers in Ukraine. Pursuant to Article 39 of the Law on Telecommunications, which regulates 'responsibilities of telecommunication operators', those operators have the responsibility:

> *7) to keep records concerning the provided telecommunication services over the duration of a period of action as established by the law of Ukraine and to provide information concerning the services having been provided following the procedure established by the law;*

In this context, we note that representatives of private sector consider data retention rules to be imprecise, unforeseeable and disproportional. In particular, it is not sufficiently foreseeable what is the scope of the phrase "records" in Article 39(7) of the Law on Telecommunications. As was already noted by Council of Europe's experts, [111] in these circumstances "*service providers are subject to vague and unforeseeable obligation, because they cannot know with certainty which data should be retained. Also, citizens have no indication which of their private data are stored and for what purposes*". Secondly, it is also concerning that data retention obligation is stipulated by reference to period of action as established by civil code, since this leads to additional vagueness and disproportionality. Finally, Law on Telecommunications does not introduce other relevant conditions and safeguards, which have developed in comparative law and practice in recent years. For all of these reasons, we emphasize once again the need to undertake relevant legislative amendments.

## 7.4 Production order

Ukraine did not implement Article 18 of the Convention as a standalone measure (specific production order). In such circumstances, Ukrainian authorities rely on Chapter 15 of the CPC, which covers "Provisional Access to Objects and Documents", to give effect to requirements arising under Convention's Article 18. Pursuant to Article 159 of the UaCPC,

> *1. Provisional access to objects and documents consists in providing a party in criminal proceedings by the person who owns such objects and documents, with the opportunity to examine such objects and documents, make copies*

[111] See Report on Ukraine on Current legislation and draft laws supplementing and amending various issues related to cybercrime and electronic evidence, November 2016.

> *thereof and, upon adoption of the appropriate ruling by investigating judge, court, seize them (execute seizure).*
>
> *2. Provisional access to objects and documents shall be executed based on a ruling of investigating judge, court.*

At this point, it is important to note that "provisional access to objects and documents" under Ukrainian legislation contains elements of both production and seizure. This follows clearly from the scope of Article 159(1) which stipulates that provisional access consists in providing party with the opportunity to (1) examine objects and documents, (2) make copies thereof and (3) seize them (execute seizure). In terms of method of provisional access, we note that, pursuant to Article 165(1) of the UaCPC,

> *The person named in investigating judge's, court's ruling on provisional access to objects and documents as the possessor of objects and documents 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.*

On the other hand, Article 165(3) also stipulates that

> *3. A person who shows an order on temporary access to things and documents is obliged to leave to the owner of the things and documents a description/list of the things and original or copies of documents that were seized to execute the order of the investigating judge, the court.*

and paragraph 4 of the same article provides that

> *At the request of the owner, a person who shows an order on temporary access to things and documents should leave a copy of seized originals documents to the owner. Copies of the seized documents or seized originals documents are made using copying technique, electronic means of the owner (with his consent) or copying equipment, electronic means of the person who shows an order on temporary access to things and documents.*

Method of "provisional access", which may include seizure, is determined by the investigator's motion. This follows from Article 160(7), which stipulates that such motion must contain:

> *7justification for the need to seize things and original or copies of documents if the matter is initiated by the party to the criminal proceedings..*

In terms of foreseeability, national stakeholders have explained that Ukrainian courts consider that computer data falls within the scope of "document", pursuant to Article 99(1) of the UaCPC, which defines a "document" as 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".*

Moreover, it is further stipulated in Article 99(2) paragraph 2 that documents might be

> *"materials of photography, sound recording, video recording and other data media (including electronic)".*

Consequently, we hold that the relevant provisions of UaCPC's Chapter 15 are foreseeable to a reasonable degree. On the other hand, it was also expressed by some national stakeholders that there is some uncertainty here since the application of relevant provisions in practice sometimes leads to different legal interpretations. In such circumstances, Ukrainian legislator might wish to make necessary notions more precise, by introducing specific notion of electronic evidence. This would also be consistent by other recommendations of the Council of Europe.[112] Also, as noted above, UaCPC does not differentiate between various categories of computer data. Hence, there are no specific rules for production of subscriber information. Addressing these shortcomings and by making appropriate amendments would also contribute to quality of legislation and consequently compliance with Article 15.

Further, we note that other conditions and safeguards are used in Chapter 15 of the UaCPC.

Firstly, provisional access to objects and documents requires court order. Pursuant to UaCPC, it can be granted by investigating judge during pre-trial investigation or to court during trial.[113] Moreover, motion to the court must be bases upon reasoned request of the investigator, which must also be pre-approved by a prosecutor. In particular, we note that Article 160(2) requires that motion to grant provisional access to objects and documents must contain:

> *4) grounds to believe that the objects and documents are or can be in possession of the physical or legal person concerned;*
>
> *5) significance of the objects and documents for establishing circumstances in the criminal proceedings concerned;*
>
> *6) possibility to use as evidence the information contained in the objects and documents, and impossibility to otherwise prove circumstances which are supposed to be proved with the use of such objects and documents, in case the motion to grant provisional access pertains to objects and documents containing secrets protected by law;*
>
> *7) substantiation of the necessity to seize the objects and documents, if such an issue is raised by a party to criminal proceedings.*

These conditions, as written, represent important safeguards against arbitrary application. On the other hand, we also note that, pursuant to Article 163 of the UaCPC, investigating judge is not required to base its ruling on all of the aforementioned conditions. Namely, pursuant to paragraph 5 of this Article,

> *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;*

[112] See Report on Ukraine on Current legislation and draft laws supplementing and amending various issues related to cybercrime and electronic evidence, November 2016.
[113] UaCPC, Article 160(1).

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

It follows from these provisions that most important element on which judicial authorization is dependent if the significance of objects and documents for criminal proceedings, which is much narrower than what is required content of investigator's / prosecutor's motion.

Requirement to demonstrate "impossibility to otherwise prove circumstances which are supposed to be proved" is applicable only to objects and documents contain "secrets protected by law". These secrets are defined in Article 162 of the UaCPC, which reads as follows:

*1. Secrets protected by law and contained in objects and documents are:*

*1) information in possession of a mass medium or a journalist and which was provided to them on condition that its authorship or source of information would not be disclosed;*

*2) information, which may constitute medical secret;*

*3) information which may constitute secrecy of notary's activity;*

*4) confidential information, including commercial secrets;*

*5) information which may constitute bank secrecy;*

*6) personal correspondence of a person and other notes of personal nature;*

*7) 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.;*

*8) personal data of an individual, which are in his personal possession or in personal database, which the possessor of personal data has;*

*9) State secret.*

Provisional access to objects and documents containing these secrets can be granted in accordance with Article 163(6) of the UaCPC:

*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.*

Moreover, we note that, pursuant to Article 161 of the UaCPC, there are some other objects and documents which are excluded from the scope of "provisional access". These include:

> *1) correspondence or any other form of communication between defense counsel and his client or any person, who represents his client, in connection with the provision of legal assistance;*
>
> *2) objects which are attached to such correspondence or any other form of communication.*

## 7.5 Search and seizure of stored computer data

There are no provisions in the UaCPC which would create specific legal framework for computer-related search and seizure. In such circumstances, Ukrainian authorities use traditional search and seizure powers as a legal basis giving effect to Article 19 of the Convention on Cybercrime. In this context, search of home or other possessions of a person (Articles 234 – 236) and Chapter 16 ("provisional seizure of property") are relevant.

Firstly, we note that search is defined as one of the investigative actions in Chapter 20 of the UaCPC. Pursuant to Article 234(1) of the UaCPC,

> *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.*

Speaking about conditions and safeguards applicable to search action, we note that UaCPC contains a general provision regarding protection of home or other possessions of a person. Namely, Article 233 provides that:

> *1. Nobody is allowed to enter home or any other possession of a person for any purpose whatsoever otherwise than upon voluntary consent of the owner or based on a ruling of investigating judge, and except in cases specified in part three of this Article.*
>
> *2. It is understood that "home" means any premise an individual owns permanently or temporarily whatever purpose it serves and whatever legal status it has, and adapted for permanent or temporary residence of physical persons, as well as all constituent parts of such premises. Premises specially intended for keeping of persons whose rights have been restricted by law, are not deemed dwellings. "Other possession of a person" refers to a vehicle, land parcel, garage, other structures or premises for household, service, business, production or other use etc., which a person owns.*

In such circumstances, search is executed on the basis of investigating judge's ruling,[114] which is made upon request of the public prosecutor or investigator (pre-approved by public prosecutor). Pursuant to Article 234(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;*

[114] UaCPC, Article 234(2).

> *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.*

Moreover, considering that search is one of investigative actions, general rules applicable to such actions are relevant here. Firstly, we note that pursuant to Article 223(4) of the UaCPC,

> *Conducting investigative (detective) actions in night-time (between 10 PM and 06 AM) is not permitted, except for urgent situations where delay in conducting investigative actions may result in the loss of traces of criminal offence or in the suspect's absconding.*

In this context, we also note that according to Article 236(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.*

Moreover, Article 223(7) requires mandatory participation of at least two witnesses of investigative action. These witnesses "may be examined during trial as witnesses of the conduct of the investigative (detective) action concerned".

Regarding seizure, we note firstly that Article 168 of the UaCPC stipulates that "property may also be provisionally seized during search…". Therefore, provisions of Chapter 16 of the UaCPC ("provisional seizure of property") are applicable. Scope of this measure is defined in Article 167(2), which reads as follows:

> *2. The property in the form of objects, documents, money, etc. may be provisionally seized if there are sufficient grounds for the belief that such property:*
>
> *1) has been found, fabricated, adapted, or used as means or instruments of the commission of criminal offence and/or preserved signs of it;*
>
> *2) has been intended (used) to induce a person him to the commission of a criminal violation, financing and/or providing material support to or as a reward for its commission;*
>
> *3) has been an object of a criminal violation related inter alia to its illegal circulation;*
>
> *4) has been gained as a result of commission of a criminal violation and/or is proceeds of such as well as any property to which they have been converted in full or in part.*

Foreseeability of the notion "documents" was already addressed above (7.4). Essentially, we consider that it is sufficiently precise and foreseeable. Next, we emphasize that Article 19(3) of the Cybercrime Convention provides for several different modalities of seizing computer data ("*seize or similarly secure a computer system or part of it or a computer-data storage medium; make and retain a copy of those computer data; maintain the integrity of the*

*relevant stored computer data; render inaccessible or remove those computer data in the accessed computer system*"). These options are not implemented adequately in UaCPC. On the other hand, there seems to be no dispute among national stakeholders that UaCPC allows law enforcement authorities to use less restrictive method. But, it is questionable whether this principle is pursued in practice. In any case, we hold that options mentioned in Convention's Article 19(3) should also be adequately reflected in the UaCPC. From the perspective of Articles 19(3) and 15 of the Cybercrime Convention, adequate solution would be the one where different modalities of conducting seizure would be clearly defined in the law, and where investigators, prosecutors and the courts would be under a legal obligation to use the method which is (in particular circumstances) the least restrictive.

Finally, we note that there are few other conditions and safeguards in the UaCPC. One of them is the obligation to make records about investigative action. Pursuant to Article 168 of the UaCPC,

> *3. During… search and provisional seizure of property or immediately thereafter, the investigator, public prosecutor, other authorized official is obliged to draw up an appropriate record.*
>
> *4. After provisional seizure of property, the authorized official is obliged to ensure preservation of such property in the procedure established by the Cabinet of Ministers of Ukraine.*

Finally, Article 169 stipulates conditions under which objects and documents must be returned:

> *1. Provisionally seized property shall be returned to the person from whom it has been seized:*
>
> *1) upon public prosecutor's resolution, if he finds that the seizure was ill-grounded;*
>
> *2) upon ruling of investigating judge or court, if it dismisses public prosecutor's motion to attach the property;*
>
> *3) in cases set forth in paragraph five of Article 171 and paragraph six of Article 170 of this Code.*
>
> *4) in cases where arrest is cancelled*

## 7.6 Real-time collection of traffic data

Section 2 of Ukrainian CPC's Chapter 21 regulates "interference in private communication", which includes several covert (detective) investigative actions (CDIA). It is unclear whether this section applies to real-time collection of traffic data, as defined in Article 20 of the Cybercrime Convention. While the text of Articles 263 and 264 might allow such interpretation, Article 258(4) nevertheless stipulates that "interference in private communication implies access to the contents of communication". In the light of these provisions, we consider that there is no proper legal basis for real-time collection of traffic data in the UaCPC. Consequently, we propose that necessary amendments are made. We also note that relevant

opinions in this matter have already been expressed by Council of Europe's experts,[115] and that proposals for legislative amendments have also been given.[116]

## 7.7 Interception of content data

### 7.7.1 Legal basis

Interception of content data is regulated by Chapter 21 of the UaCPC, which covers covert investigative actions. Within these measures, Section 2 (Articles 258 *et seq*.) regulate "interference in private communication". Pursuant to Article 258(4), "the following shall be types of interference in private communication:

> *2) arrest, examination and seizure of correspondence;*
>
> *3) collecting information from telecommunication networks;*
>
> *4) collecting information from electronic information systems".*

Firstly, we note with satisfaction that UaCPC limits the application of "arrest, examination and seizure of correspondence" to correspondence using material mediums, and does not include any type of communication in electronic form. Namely, pursuant to Article 261(4),

> *Correspondence referred to in the present Article shall include letters of all types, postal packets, parcels, postal containers, postal money orders, telegrams, and other material mediums for exchange of information among individuals.*

Next, Article 263(1) of the UaCPC defines so-called "collecting information from transport telecommunication networks", in the following terms:

> *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.*

Finally, Article 264(1) of the UaCPC defines measure of "collecting information from electronic information systems". Pursuant to this provision,

> *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*

[115] See Report on Ukraine on Current legislation and draft laws supplementing and amending various issues related to cybercrime and electronic evidence, November 2016.
[116] See Expert Opinion on Draft amendments to the legislation of Ukraine concerning cybercrime and electronic evidence, May 2017.

*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.*

### 7.7.2 Authorization procedure

Ukrainian CPC requires authorization of the investigating judge to undertake covert investigative (detective) actions mentioned above.[117] Moreover, these decisions fall under the competence of limited number of courts, namely "Appeals Court of the Autonomous Republic of Crimea, appeals court of oblasts, cities of Kyiv and Sevastopol, within the territorial jurisdiction of which the pre-trial investigative agency concerned is located".[118]

Urgent authorization procedure is regulated by Article 250 of the UaCPC ("conducting a covert investigative (detective) action before investigating judge adopts a ruling"). This article reads as follows:

*1. In the exceptional and urgent cases related to saving human life and preventing the commission of grave or especially grave crime as provided for by Sections I, II, VI, VII (arts. 201 and 209), IX, XIII, XIV, XV, XVII of the Special Part of the Criminal Code of Ukraine, a covert investigative (detective) action may be initiated before investigating judge adopts a ruling in the cases anticipated for in this Code, upon decision of investigator approved by prosecutor, or upon decision of public prosecutor. In such a case, public prosecutor shall be required to immediately after the initiation of such covert investigative (detective) action, apply to investigating judge with an appropriate request.*

*2. Investigating judge considers this request in accordance with the requirements of Article 248 of the present Code.*

*3. Carrying out any activities related to conducting a covert investigative (detective) action should be immediately discontinued if the investigating judge passes a ruling denying permission to conduct the covert investigative (detective) action concerned. Information obtained as a result of conducting such covert investigative (detective) action is subject to destruction as prescribed in Article 255 of the present Code.*

Urgent authorization procedure, as regulated in the UaCPC, contains sufficient safeguards to protect against abuse of this procedural power. Next, we look at the authorization authority's scope of review. As explained in the introduction, the ECtHR has held that this authority it must be capable of verifying (1) the existence of a reasonable suspicion against the person concerned, and (2) whether the requested interception meets the requirement of "necessity in a democratic society", which implies that the aim pursued by law enforcement authorities cannot be achieved by less restrictive means. The purpose of this is to ensure that "*secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration*".[119]

[117] See Article 263(1) and 264(1) of the UaCPC.
[118] UaCPC, Article 247.
[119] Zakharov v Russia, ECtHR app. no. 47143/06, para 257.

Regarding these conditions, we note first that pursuant to Article 246(2) of the UaCPC, "covert investigative (detective) actions are conducted if information on criminal offence and its perpetrator cannot be obtained otherwise". Next, Article 248(2) of the UaCPC "examination of the request to obtain permission for the conducting of a covert investigative (detective) action") stipulates that request submitted to the investigating judge must contain:

> *2) brief description of the circumstances of the crime within the framework of investigation of which the request is filed;*
>
> *4) information on the individual (individuals), place or object in whose respect it is necessary to conduct covert investigative (detective) action;*
>
> *5) circumstances that provide grounds for suspecting the individual of committing the crime;*
>
> *6) type of covert investigative (detective) action to be conducted, and substantiation of the time limits for the conducting thereof;*
>
> *7) substantiation of impossibility to obtain otherwise knowledge on crime and the individual who committed it;*
>
> *9) substantiation of the possibility to obtain in the course of conducting of covert investigative (detective) action, of evidence which, alone or in concurrence with other evidence, may be significantly important for the clarification of the circumstances of crime or the identification of perpetrators thereof.*

From this provision, it is obvious that interception request must contain all elements needed to establish the existence of a reasonable suspicion against a person and necessity of conducting this action. On the other hand, it seems that judge's scope of review is limited. Namely, pursuant to Article 248(3) of the UaCPC,

> *3. Investigating judge passes a ruling to allow conducting the requested covert investigative (detective) action if the public prosecutor proves that sufficient grounds exist that:*
>
> *1) a crime of relevant severity has been committed;*
>
> *2) in the course of covert investigative (detective) action, information is likely to obtained, which alone or in totality with other evidence may be of essential importance for establishing circumstances of the crime or identification of perpetrators thereof.*

We note here that Article 248(3) does not require that prosecutor proves necessity, i.e., "impossibility to obtain otherwise knowledge on crime and the individual who committed it". This conclusion is also confirmed by Article 248(4), which stipulates that "investigating judge's ruling to allow conducting a covert investigative (detective) action should meet general requirements for judicial decisions as prescribed in the present Code, as well as contain information on:

> *1) public prosecutor, investigator who applied for permission;*
>
> *2) criminal offence which is subject of pre-trial investigation within which the ruling is passed;*

*3) person (persons) place or object targeted by the requested covert investigative (detective) action;*

*4) type of the covert investigative (detective) action and information depending on the type of investigative (detective) action, on identification signs which will allow to uniquely identify the subscriber under surveillance, transport telecommunication network, and terminal equipment etc.;*

*5) time in which the ruling is valid".*

During the discussions, national stakeholders have explained that investigative judges in practice require that prosecutors elaborate upon "impossibility to obtain otherwise knowledge on crime and the individual who committed it". However, we consider that it is important that this element is explicitly included among those whose existence judge must establish (Article 248(3)). It is moreover equally important that judges are required to elaborate upon (give reasons for) this requirement in their ruling (Article 248(4)). This is consistent with opinions and recommendations which have, in this context, already been expressed by Council of Europe's experts.[120]

## 7.7.3 Scope of application

As explained in the introduction, international law requires that domestic legislation restricts the application of interception measures in relation to a limited range of serious criminal offences. Moreover, it requires also that national law defines with precision categories of people liable to have their communications intercepted.

Regarding the first of these conditions, we recognize that Article 246(2) of the UaCPC stipulates that covert investigative (detective) actions mentioned above (7.7.1) can be conducted exclusively in criminal proceedings in respect of grave crimes or crimes of special gravity. Consequently, we hold that Ukrainian legislation adequately limits the application of interception, in relation to seriousness of criminal offences.

Next, regarding categories of people liable to have their communications intercepted, we note that this issue is addressed only by a provision which stipulates that the request to obtain permission for the conducting of a covert investigative (detective) action must contain "circumstances that provide grounds for suspecting the individual of committing the crime". We are not confident that this provision is sufficient to ensure adequate protection. Consequently, we propose that this issue be addressed in the future, and that UaCPC stipulates explicitly which categories of persons can be subject to relevant covert investigative (detective) actions.

Finally, we note that pursuant to Article 258(4)(5), "interference in private communication of defense counsel, between clergyman and the suspect, accused, convict, acquitted shall be forbidden".

## 7.7.4 The duration of interception

[120] Expert Opinion Prepared by independent Council of Europe experts Marko Juric, Nigel Jones and Markko Künnapu with the support of the Cybercrime Programme Office of the Council of Europe, on Draft amendments to the legislation of Ukraine concerning cybercrime and electronic evidence, May 2017.

Article 15(2) calls also for limitations of the duration of certain procedures, and the same requirement is expressed by the ECtHR. Moreover, as stated by the ECtHR, there should exist "*a clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled*".[121]

In the UaCPC, duration of investigative (detective) actions is defined in its Article 249, which reads as follows:

> *1. Time in which the investigating judge's ruling to allow conducting a covert investigative (detective) action may not be valid for more than two months.*
>
> *2. If investigator, public prosecutor finds it necessary to extend conducting a covert investigative (detective) action, the investigator upon approval of public prosecutor, or public prosecutor may apply to the investigating judge for making a new ruling under Article 248 of the present Code.*
>
> *3. In addition to information specified in Article 248 of the present Code, investigator, public prosecutor shall be required to provide additional information which provide grounds for extending the conducting of covert investigative (detective) action.*
>
> *4. The aggregate duration of a covert investigative (detective) action in one criminal proceeding given permission of investigating judge, may not exceed the maximum duration of pre-trial investigation as set forth in Article 219 of this Code. In case where such investigative (detective) action is conducted to locate an individual hiding from the pre-trial investigation authority, investigating judge or the court or being searched, it may last until the wanted individual is located.*
>
> *5. Public prosecutor shall be required to take decision to discontinue conducting of a covert investigative (detective) action if such action is no longer needed.*

In our opinion, conditions and safeguards mentioned above are sufficient to ensure protection against abuse of the law.

## 7.7.5 Notification

> *Article 253. Notifying individuals in whose respect covert investigative (detective) actions have been conducted*
>
> *1. Individuals whose constitutional rights were temporarily restricted during conducting covert investigative (detective) actions, as well as the suspect, his/ her defense counsel shall be informed about such restriction in written form by public prosecutor or, upon his instruction, by investigator.*
>
> *2. Specific time of notification shall be chosen taking into account the presence or absence of possible risks for the attainment of the objective of pre-trial investigation, public security, life or health of individuals who are involved in the conduct of covert investigative (detective) actions. Appropriate notification*

[121] Zakharov v Russia, para 250.

> *of the fact and results of covert investigative (detective) actions shall be required to be made within twelve months since the date of termination of such actions, but not later than an indictment has been produced to court.*

In our opinion, conditions and safeguards mentioned above are sufficient to ensure protection against abuse of the law.