CyberEast
Action on Cybercrime for Cyber Resilience
in the Eastern Partnership Region

Updated study (2023)

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

Prepared by a Council of Europe expert
under the CyberEast Project

Co-funded
by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Co-funded and implemented
by the Council of 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 expert Marko Jurić 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

1.1 Procedural powers in the Convention, their scope and purpose

Convention on Cybercrime is built on three main set of rules: (1) substantive criminal law, (2) procedural law and (3) international cooperation. Chapter 2, Section 2 of the Convention, 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 crime by facilitating its detection, investigation and prosecution. It is important to note here that these powers go beyond investigations of cybercrime. Pursuant to Article 14(2) of the Convention, the abovementioned procedural powers must be applicable to investigations and prosecutions of:

a) the criminal offences defined in the Convention, and

b) other criminal offences committed by means of a computer system; and

c) the collection of evidence in electronic form of a criminal offence.

The point c here makes it unambiguous that procedural powers defined in the Convention are meant to be used in any criminal investigation and/or prosecution, and not just in those involving cybercrime.

It is important to note here that the Convention envisages the abovementioned procedural powers as tools to be used for specific criminal investigations and prosecutions. It does not deal with the preventive actions which the state might be undertaking to reduce criminal activities, nor does it cover the use of those procedural powers for other aims and purposes (for instance protection of national security, intelligence purposes, other police duties, etc.).

1.2 Human rights mandate of the Convention

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:

   i. Incorporate the principle of proportionality – Article 15(1),

   ii. 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

   iii. 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 analyse 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:

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

c) 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.

   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).

1.3 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

[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.

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 analysing 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.

1.4 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. 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 analysing 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.

4) Whether there are any categories of privileged data or information which are excluded from the scope of production order.[6]

5) Also in this context, we note that there is no consensus that judicial authorization should be required for this power.[7]

1.5 Search and seizure of stored computer data

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

[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).

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.

1.6 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.

1.7 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 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]

[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.
[13] Zakharov v Russia, para 231.
[14] Zakharov, para 231.

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

1.7.1 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.

1.7.2 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:

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]

[15] Zakharov v. Russia, para 257.
[16] Zakharov v. Russia, para 257 and other cases quoted there.
[17] Zakharov v. Russia, para 260 and other cases quoted there.

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]

1.7.3 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.

1.7.4 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 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]

1.7.5 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

[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.
[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.

which are not relevant to the purpose for which they have been obtained must be destroyed immediately.[24]

1.7.6 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".

1.7.7 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".

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".

1.7.8 Effective oversight of secret surveillance of communications

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

It is very well established in the case-law of the ECtHR that since surveillance of communications is exercised in secret, the risks of abuse and arbitrariness are significant.[26] It is therefore necessary that the state implements adequate safeguards against arbitrary application and abuse of secret surveillance powers. As explained by the ECtHR, "the overarching requirement is that a secret surveillance system must contain effective guarantees – especially review and oversight arrangements – which protect against the inherent risk of abuse, and which keep the interference which such a system entails with the rights protected by Article 8 of the Convention to what is "necessary in a democratic society"".[27]

In general, we can differentiate between supervision of oversight in specific cases, which is usually within the competence of authorising judges, and general oversight of the operation of secret surveillance system as such. This second issue is of relevance here.

National practices of European countries regarding oversight of these services vary greatly, but some important and common characteristics can be identified. In this context, in addition to the mandatory standards established by the ECtHR, there is very useful guidance by the *Council of Europe's Commissioner for Human Rights* and the *Venice Commission*.

In general, the functioning of secret surveillance system should be subject to effective oversight of one or more supervisory authorities. As noted by the Council of Europe's Commissioner for Human Rights, member states of the Council of Europe should designate "one or more bodies that are fully independent from the executive and the security services to oversee all aspects of security service regulations, policies, operations and administration".[28] The ECtHR has further set the standards by emphasizing that the relevant factors for deciding whether the oversight arrangements are adequate are (a) the independence of the supervisory authorities, their competences, and their powers (both to access materials and to redress breaches, in particular order the destruction of surveillance materials), and (b) the possibility of effective public scrutiny of those authorities' work.[29]

Further, when assessing the position, independence, and powers of oversight authorities the ECtHR considers factors such as:

- Whether the oversight authorities are sufficiently independent *vis-à-vis* the authorities which they must oversee. In this context, security vetting by security services for members of oversight bodies might become an issue, if that body is in charge of overseeing security service operations. While this is not fully excluded, appropriate steps must be undertaken to guarantee independence of members of oversight bodies.[30]
- Practice of electing professionals from law enforcement and intelligence sectors as members of oversight bodies and their later return to the service ("revolving door") is seen as problematic.[31]

[26] Zakharov v. Russia, paragraph 229.
[27] Ekimdzhiev and Others v. Bulgaria, paragraph 292.
[28] Council of Europe Commissioner for Human Rights, Democratic and effective oversight of national security services, 2015, p. 11.
[29] Ekimdzhiev and Others v. Bulgaria, paragraph 334.
[30] Ekimdzhiev and Others v. Bulgaria, paragraph 340 *et seq*.
[31] Ekimdzhiev and Others v. Bulgaria, paragraph 339 *et seq*.

- Members of the oversight bodies should have necessary legal and other expertise to undertake their tasks.[32]
- Oversight body should have necessary competences, including unfettered access to all relevant materials and power to undertake on-site inspections.[33]
- Oversight bodies should have the competence to order remedial measures, such as the destruction of surveillance materials.[34]

[32] Ekimdzhiev and Others v. Bulgaria, paragraph 342.
[33] Ekimdzhiev and Others v. Bulgaria, paragraph 343.
[34] Ekimdzhiev and Others v. Bulgaria, paragraph 344-345.

2 Armenia

2.1 Relevant legal framework

This part of the report is based on the analysis of the following statutory law of Armenia:

1. Armenian Code on Criminal Procedure (hereinafter: AmCPC) [35]
2. Armenian Law on Operative-Intelligence Activity (hereinafter: AmLOIA) [36]

There have been significant changes in the legislation of Armenia after the last report on the implementation of Article 15 of the Convention. Most importantly, the Code of Criminal Procedure was substantially changed and the new version of it was enacted on June 30, 2021. It became operational in full on January 1, 2023. Also, the Law on Law on Operative-Investigative Activity, first enacted in the current version in 2007, was amended multiple times, most recently in 2023.

The purpose of this report is overall analysis of national legislation in the implementation of procedural powers of the Convention (Articles 16 to 21), from the perspective of conditions and safeguards used to ensure protection of fundamental human rights and freedoms (Convention's Article 15). And since the procedural powers in the Convention are used to collect evidence for the purpose of specific criminal investigations or proceedings (Article 14), the primary relevant sources of regulation in the domestic law are codes on criminal procedure. But, there are many secondary issues which can be regulated by other laws as well, and hence we attempted to pursue a broader approach and also look into those sources. Nevertheless, the analysis made here is limited to conditions and safeguards applicable to actions undertaken broadly in the context of criminal proceedings. Use of procedural powers for national security, intelligence and other purposes was not analysed.

2.2 General considerations

2.2.1 Applicable national legislation

As is the case in other jurisdictions analysed in this report, in Armenia procedural powers which correspond to those in the Convention are regulated by two sets of legal provisions, namely the ones in the AmCPC and the ones in the AmLOIA. The main difference seems to be that the AmCPC regulates investigations and prosecutions of specific criminal offences, while the AmLOIA is broader in the sense that powers defined therein are used generally to "protect human and citizen's rights and freedoms, state and public security from illegal encroachments".[37] More specifically, Article 4 of the AmLOIA contains a broad list of the goals of operative-investigative activity, which go beyond investigations of particular crimes and include state activities to prevent and supress crime, detect persons attempting to commit criminal offences, undertaking measures necessary in the context of security vetting procedures, protecting market competition, etc. This is also reflected in the broad designation of authorities empowered to undertake operative-investigative actions, which includes the police, military police, national

[35] Available at https://www.arlis.am/DocumentView.aspx?DocID=176081.
[36] Available at https://www.arlis.am/DocumentView.aspx?docID=152666.
[37] AmLOIA, Article 3.

security bodies, tax authorities, customs authorities, and penitentiary service. The key issue for the purposes of our analysis is relationship between power in the AmLOIA and those undertaken on the basis of the AmCPC, and whether both sets of rules provide for adequate protection of fundamental human rights and freedoms.

When it comes to the collection of evidence for the purpose of criminal proceedings, Article 86(2) of the AmCPC generally stipulates those documents compiled, and data recorded as a result of operative-investigative measures, are not evidence in criminal proceedings. But it is obvious from other provisions of the AmCPC that operative-investigative measures can be undertaken in the context of criminal proceedings also pursuant to the AmLOIA. For instance, Article 188 of the AmCPC stipulates that:

- operative-investigative measures within the framework of the investigation may be carried out by the investigator's instruction or at the initiative of the investigative body, and that
- the results of secret investigative activities and operative-investigative measures performed within the framework of the investigation are immediately presented to the investigator, and that
- at the end of the preliminary investigation, the ongoing secret investigative activities and operative-investigative measures are stopped.

Moreover, Article 96(3) clarifies that video recordings, sound recordings and other objective documents obtained with the permission of the court as a result of operative-investigative activities carried out outside the framework of criminal proceedings can be recognized as non-procedural documents and attached to the proceedings materials only in the event that the relevant measure was implemented to prevent or disrupt the crime, or in order to identify the perpetrator at the time of the commission of the crime or immediately after it.

Likewise, AmLOIA prescribes in its article 40(1) that the results of operative-investigative activities, obtained in accordance with the procedure established by this law, are evidence (with some exceptions).

If our understanding of these provisions is correct, this means that (in addition to the exception under Article 96(3) of the AmCPC) procedural powers relevant to those prescribed in Articles 16 to 21 of the Convention will only result in legally admissible evidence if they are executed on the basis of the AmCPC, or if they are executed on the basis of the AmLOIA in the framework of criminal proceedings initiated pursuant to the AmCPC. While this interpretation would generate less issues from the human rights perspective, it would be best if it was clearly set in law. Hence, national authorities of Armenia might want to consider this and ensure that the law defines in a completely clear and foreseeable way in which circumstances national authorities are acting on the basis of a specific law. For instance, it should not be the case that interception of communications can be ordered in the context of criminal proceedings on the basis of two laws, which contain at least in part different conditions for its authorization.

2.2.2 Status of electronic evidence

Armenian legislation recognizes multiple types of evidence (AmCPC Article 86), including "external documents". These are "any written, digital, graphical or other written record on a

paper, magnetic, electronic or other medium containing data about the facts important for the criminal proceedings, which was formed outside the scope of the given criminal proceedings" (Article 96(1) of the AmCPC). Hence, it is regulated in a reasonably foreseeable way that electronic evidence is admissible under the AmCPC.

2.2.3 Categories of computer data recognized in the legislation

There is no proper differentiation in the AmCPC between different types of computer data (i.e., subscriber information, traffic data and content data). All these categories can fall within the broad notion of "document" as is regulated by Article 96(1) of the AmCPC. Also, as will be seen below in the report, there is also no proper differentiation between surveillance powers in the domain of electronic communication. Consequently, acquisition of traffic data and content data is covered by the same legal provisions.

2.3 Expedited preservation of stored computer data

In our analysis of the new AmCPC we did not identify provisions which would seek to implement Article 16 of the Convention. There is very limited number of provisions which mention preservation of all. One of them is Article 99 of the AmCPC, which deals with the "preservation of documents". But this article only covers issues related to keeping (i.e., storing) of documents within the framework of criminal proceedings and does not correspond to the subject-matter of Article 16 of the Convention. AmCPC stipulates that the investigative body generally has the power to "preserve objects and documents important for criminal proceedings".[38] But, when it comes to preservation of computer data, there seem to be no specific legal ground for the implementation of this power.

Hence, the situation regarding Article 16 remains largely unchanged compared to 2018 report. Armenian legislation still does not recognize expedited preservation of stored computer data (Article 16 of the Convention) as a standalone measure. To be sure, there have been then and continue to exist some 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 the context of criminal proceedings.

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 (provided that 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. Also, this is a requirement of the new AmCPC from 2021. As mentioned above, there is a general duty of investigative and prosecutorial bodies to minimize interferences with personal liberty and integrity. Pursuant to

[38] Article 42(1)(8) of the AmCPC.

Article 18 of the AmCPC, when choosing a coercive measure against a person, the body implementing the procedure is guided by the principle of minimum. But it is not possible to pursue this approach if there is no suitable procedural power to be used.

Finally, the lack of preservation powers will also negatively impact efforts of Armenian authorities in the context of international cooperation.

For all of these reasons, we continue to insist that 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.

2.4 Expedited preservation and partial disclosure of traffic data

Unfortunately, in our review we did not identify any provision in the AmCPC which would be aimed at implementing Article 17 of the Convention. The same is true for the AmLOIA as well. The only power in the AmLOIA which might be relevant here is the "acquisition of operational information", defined as "the collection of information on persons and facts of operational interest for the purpose of implementing the tasks of operational-intelligence activity". But this power also speaks about acquisition of information and not about preservation. So even if it would be used to this purpose, it would not be in line with Article 16 of the Convention.

Hence, there continues to exist the need to implement precise and foreseeable rules regarding preservation of traffic data and/or their retention would contribute significantly to the quality of Armenian legislation. This is also of relevance for the ability of Armenian legislation to participate adequately in international data exchanges, following Convention's rules on international cooperation.

2.5 Production order

2.5.1 Production order for computer data in general

We did not identify provisions of the AmCPC which would be aimed specifically at implementing Article 18 of the Convention in part where it relates to the production of computer data in general.

2.5.2 Production order for subscriber information

Some aspects of Article 18's subject-matter seem to be at least partially covered by Article 232 of the AmCPC, which regulates "request for information". This is one of the investigative actions in the AmCPC. Third paragraph of this article empowers the investigator to, with the approval of the supervising prosecutor, request:

1. telephone numbers of those who communicate through a fixed or mobile telephone network, personal data of the subscriber of the telephone number;

2. the data necessary to find out the location of the communicators and their movement at the time of starting the telephone communication and during it;

3. the place, time and duration of connecting to the Internet and leaving the Internet, the personalization data of the Internet user or subscriber, the telephone number by which he connects to the public telephone network, the Internet address, including the Internet Protocol (IP) address, the personalization data of the recipient of the Internet phone call.

With regard to first point above, the notion of "personal data of the subscriber" is not self-evident and might therefore be defined in the legislation. Namely, the reason for this is that it can cover many different categories of information, starting from the basic identifying information and possibly including other categories of data. Hence, it is recommended that national authorities consider clarifying the meaning of this.

Second point above does not raise any issues from the perspective of legal clarity, since it is reasonably foreseeable from the provision which data are collected.

In the third point, the term "personalization data of the internet user or subscriber" seems a bit vague, at least in the English translation of the AmCPC. National authorities might want to consider this and possibly provide more specific indicators as to what those data might be.

Overall, it can be concluded that Article 232 covers partially information which, in the nomenclature of the Convention, fall within the notion of "subscriber information", and partially those which can be classified as "traffic data". This is also one of the shortcomings of this provision, since it is not entirely appropriate to treat subscriber information under the same set of rules as traffic data.

Since the request for information is one of the investigative actions in the AmCPC, conditions and safeguards applicable to those actions are valid here as well. These include:

- There need to exist sufficient grounds to believe that as a result of it, evidence important for the given proceedings can be obtained.[39]
- Power is authorized by the supervising prosecutor[40]
- Additional safeguards, described below in relation to search and seizure, are also applicable.

When it comes to the information about location of people who communicated via telephone, there is a safeguard in the AmCPC in that such information can only be requested (1) about the natural person regarding whom there are facts testifying to the commission of an alleged crime, (2) against the accused and (3) against the victim or the witness, if it is necessary to check their testimony. It is also important to note that under the principle of presumption of innocence, which is recognized as one of the main principles of the AmCPC (Article 17), the accused is not obliged to show any support to the body conducting the criminal proceedings. We consider all of these provisions to be useful safeguards in the domestic legislation.

[39] AmCPC Article 209(1).
[40] AmCPC Article 232(3).

2.6 Search and seizure of stored computer data

Contrary to the situation in 2018, when there have been no provisions in the AmCPC which would create specific legal framework for computer-related search and seizure, this matter is now regulated in more detail. The following provisions are relevant:

- Article 236 of the AmCPC which regulates "digital search". This institute is a part of general rules pertaining to the search and seizure (Article 234 et seq.).
- Article 236 of the AmCPC which regulates seizure, including the one of digital data or documents.

Both powers are considered ordinary investigative actions, which are regulated by Chapter 29 of the AmCPC. In addition to these, AmCPC also regulates secret (undercover) investigative actions (Chapter 30). Moreover, ordinary investigative actions can be further differentiated pursuant to legal grounds for their application. In essence, the key issue here is which body authorizes the execution of the measure. In general, AmCPC differentiates between investigative actions ordered by (1) Investigator, (2) Prosecutor and (3) Court. It is important to note here that per specific rules in the AmCPC (Article 209 paragraph 4), actions authorized by the Court include the

- "Digital search", and the
- Seizure of the digital data contained in the electronic devices or media, and the
- Seizure of the digital data contained in the electronic devices or media.

Finally, secret (undercover) investigative actions are performed on the basis of court decision (Article 242 paragraph 2). It therefore follows that Armenian legislation, when it comes to the authorization procedure, rightly considers search and seizure as equally serious as secret investigative powers.

Search is, pursuant to the AmCPC, an operation performed to find objects, materials, documents, or data important for the proceedings.[41] Considering that the notion of document 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. This was the case already in 2018, and the provisions of the new AmCPC only clarified this issue further. Namely, AmCPC currently in force introduced the specific notion of "digital search", which seems to directly relate to subject matter of Convention's Article 19.

Article 236 of the AmCPC defines "digital search" as the search for digital data contained in electronic devices or media.[42] It is further stipulated that data important for the proceedings are seized by copying to another medium, ensuring the integrity of data as well as the integrity of the copies which are made.

Pursuant to these provisions, general precondition for the search is that there are sufficient grounds to believe that it will result in obtaining evidence important for the given proceedings.[43] Formally, the so-called digital search, as well as search and seizure in the apartment, is

[41] AmCPC, Article 234(1).
[42] AmCPC, Article 236(1).
[43] AmCPC, Article 209(1).

authorized by the court.[44] If follows from this, as well as from Article 236, that the court order must identify data which is object of the search. In addition to this, investigators are also authorized pursuant to Article 236(3) to seize also that data which, while not being mentioned in the court warrant, by their nature or content may be related to either the crime which is the reason for the search, or another crime.

During this review, we did not identify provisions pertaining to extended search, as it is regulated by the Article 19(2) of the Convention. Hence, this issue remains unforeseeable and consequently problematic from the perspective of legal certainty.

Turning now to the Article 19(3) of the Cybercrime Convention, which provides for several different modalities of seizing computer data, we note that it is not implemented adequately in Armenian CPC. Compared to the situation in 2018, the AmCPC now additionally stipulates that "data important for the proceedings are taken by copying to another medium, ensuring the integrity of these data and the copies made from them". But, where the Convention stipulates clearly that the power to undertake includes powers to (1) seize or similarly secure a computer system or part of it or a computer-data storage medium; (2) make and retain a copy of those computer data; (3) maintain the integrity of the relevant stored computer data; and (4) render inaccessible or remove those computer data in the accessed computer system, AmCPC is not equally exhaustive and precise. According to explanations given by national stakeholders already in 2017, 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). Hence, there seems to be no dispute whether the 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 the 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 methods 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. This would also give substance to the principle defined in Article 18 of the AmCPC pursuant to which, when choosing a coercive measure against a person, the body implementing the procedure is guided by the principle of minimum.

From a legal viewpoint, there are multiple conditions and safeguards which need to be fulfilled to undertake lawful search. Some of these result from the application of general rules for the execution of investigative actions:

- Actions need to be performed by competent persons.[45]
- Investigative actions are videorecorded by default. The exception is the objective impossibility of videorecording, in which case it is necessary to involve at least two witnesses to its execution.[46] There are detailed technical rules for videorecording of investigative actions and the technical equipment used for that purposes.[47]

[44] AmCPC, Article 209(4).
[45] AmCPC, Article 210(1-4).
[46] AmCPC, Article 210(5).
[47] AmCPC, Article 214.

- In principle same investigator cannot participate in more than one investigative operation performed during the same proceeding.[48]
- Investigative actions are in general performed only during daytime.[49]
- There are detailed procedural rules regulating necessary information and warnings to be provided, rules for protection of dignity of searched persons, obligation to maintain secrecy and the rules regarding making the search protocol.[50]
- Additional protection is given in cases involving minor, incapacitated persons of persons with mental health problems;[51] as well as persons with deafness, muteness, or serious illness.[52]

Additionally, rules specific for the legality of the search are also stipulated in the AmCPC:[53]

- Legal owner of the object of search, or his representative, must be informed about the search and has the right to be present while it is undertaken. This also includes the right to observe all actions undertaken during the search and to make statements which must be entered into the record.
- He has the right to receive decision authorising the search before it is initiated.
- The investigator must take measures to prevent damage to the object(s) of the search.
- There are additional rules regulating the content of the search protocol.[54]

2.7 Surveillance of electronic communications

At the time of the last review, in 2018, there was no distinction between the real-time collection of traffic data and interception of content data in Armenian law. At that time, both measures could have been undertaken on the provisions on interception valid at that time. In other words, power to collect traffic data was in a sense implied in the power to intercept content of the communications. Situation in 2023, after the enactment of the AmCPC from 2021, largely remains the same. There is still no strict differentiation between real-time collection of traffic data and interception of content data.

2.7.1 Duties of service providers to assist in the surveillance of communications

Armenian legislation does not define in too detail methods of conducting secret surveillance of communications. On the side of the AmCPC, it is stipulated in Article 249(4) that the telecommunications organizations are obliged to provide technical systems and create other conditions necessary for the performance of the secret investigative operation at the request of the competent authorities. Moreover, pursuant to Article 242(4) of the AmCPC, the Government

[48] AmCPC, Article 210(6).
[49] AmCPC, Article 211(1).
[50] AmCPC, Article 211(2-6); Article 215.
[51] AmCPC, Article 212.
[52] AmCPC, Article 213.
[53] AmCPC, Article 234.
[54] AmCPC, Article 238.

approves the list of special technical means used during the performance of secret investigative operations. This list was made public and came into force on 1 July 2022.[55]

On the other side, AmLOIA stipulates in Article 9 that interception of communications falls under the competence of "service functioning within the system of the republican national security body of the Republic of Armenia", which acts 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".[56] 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.*
>
> *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.*

[55] According to Government's decision of 8 April 2022, effective from 1 July 2022, available at https://www.arlis.am/DocumentView.aspx?docid=161844, special technical measures used in the performance of secret investigative actions include:
1. Technical (including software) means specially designed for secret (cryptic) video surveillance and eavesdropping of apartments or other premises, monitoring and recording of events and conversations taking place in them, as well as standard technical, including software means, which are adapted or additionally developed (modified) for these purposes;
2. Technical (including software) means specially designed to penetrate computer networks and systems without a trace, to extract (change, destroy) and fix the information entered, stored, processed or transmitted in them, as well as standard technical, that including software tools adapted or additionally developed (modified) for these purposes;
3. Technical (including software) means specially designed for opening and later restoring (closing) original mechanical, electromechanical, electronic and other locking devices without keys, as well as standard technical, including software means, which adapted or additionally developed (modified) for these purposes;
4. Technical (including software) means, which are specially designed for the secret (cryptic) operation of telephone (fixed, mobile and other types of communication) conversations or messages (SMS, MMS, fax, e-mail messages, etc.) on the Internet. for monitoring, eavesdropping and recording, as well as standard technical, including also software, adapted or additionally developed (modified) for these purposes;
5. Technical (including software) means specially designed for secret (cryptic) control of correspondence, postal, telegraphic and other communications, with traceless opening and restoration of the envelope, package (outer membrane) or without opening, as well as standard technical means, including software tools that are adapted or additionally developed (modified) for these purposes;
6. Technical (including software) means specially designed for the installation of invisible signs identifying objects (banknotes, items, packages, documents, etc.), as well as standard technical, including also software means, adapted or additional are developed (modified) for these purposes.
7. Technical (including software) means specially designed for mobile and non-mobile (stationary) radiolocation, as well as standard technical, including software means, adapted or additionally developed (modified) for these purposes.
8. Technical (including software) means specially designed for secret (cryptic) examination of things and documents, as well as standard technical, including software means, adapted or additionally developed (modified) for these purposes.
9. Technical (including also software) means specially intended for covert (cryptic) monitoring of the movement of persons, vehicles and other objects, as well as standard technical, including also software means, adapted or additionally developed (modified)) are for these purposes.

[56] AmLOIA, Article 9(5).

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 by relevant authorities. 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.

2.7.2 Real-time collection of traffic data

In the new AmCPC Article 249 regulates surveillance of "digital, including telephone communications". But, once again, it seems that the text of this provision refers only to the content of the communications and that specific reference to traffic data is avoided.[57]

On the contrary, AmLOIA is more detailed when it comes to surveillance of communications. Relevant provision of the AmLOIA in this context is its article 26, which covers monitoring of conversations via telephone, Internet telephone and generally electronic communication means.

Compared to the AmCPC, AmLOIA is more precise when it comes to the object of the monitoring, in the sense that it clearly stipulates categories of data which can be obtained on the basis of Article 26. In the first step, AmLOIA differentiates between communication via (1) fixed telephone network, (2) mobile telephone network and (3) Internet communications.

For fixed and mobile telephone network, surveillance order pursuant to Article 26 covers content data and the following categories of metadata: telephone numbers, data necessary to determine the date, start and end of the telephone conversation and telephone number to which the call was eventually forwarded.

For Internet communication, surveillance on the basis of Article 26 of the AmLOIA covers content data and data through which relevant authorities can be determine (1) geographic location, day, time and duration of Internet connection and disconnection, including IP (Internet Protocol) address; (2) Internet user or subscriber name and personalization data (user ID), and (3) the telephone number by which he connects to the public telephone network, the Internet address, the name of the recipient of the Internet telephone call, or every other information about the facts, events, circumstances relating to that person in such a form that allows or may allow to identify his identity.

Therefore, it is clear that the AmLOIA enables collection of traffic data under the same set of conditions as interception of content data.

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

[57] In the Convention, traffic data is defined as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service". See Article 1(d) of the Convention.

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.

2.7.3 Interception of content data

2.7.3.1 Legal grounds for interception of content data

As explained above, in Armenian legislation some investigative powers are covered by both the AmCPC and the AmLOIA. Surveillance of communications is one of those powers. We use the broad notion of "surveillance of communications" here because, as explained above, Armenian legislation does not differentiate between (real-time) collection of traffic data and interception of content data.

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.[58] 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 Republic of Moldova.[59] Similar solution can be found in Article 7(3) of the Georgian Law on Operative Investigatory Activities.[60]

In the context of the AmCPC, surveillance of communications is regulated as one of the secret investigative actions in Article 249. Pursuant to this provision, surveillance of digital communications encompasses different modes of communication, including (1) fixed telephony, (2) mobile telephony and (3) internet communications. In all cases, object of the surveillance is the communication's content. For mobile telephony, it is elaborated in more detail that the content includes telephone conversation, text, image, sound, video, and other messages. Likewise, for internet communication, it is also stipulated that the term includes IP telephone communications and "electronic messages". These are all useful clarification which contributes to the foreseeability of the law. It also appears that some metadata, such as telephone numbers involved in the communication as well as dates and times of the communication may also be recorded on the basis of this provision. But there is no doubt that the direct object of the surveillance here is the content of the communication, and hence this provision corresponds to the one required under Article 21 of the Convention.

On the other side, relevant provision in the AmLOIA seems to be Article 26, which covers monitoring of telephone conversations. But the title of the article is slightly misleading here,

[58] Article 4 of the AmLOIA.
[59] See chapter 6.7.1 below.
[60] See chapter 5.7.1 below.

since the provision covers, similarly as the AmCPC, (1) fixed telephony, (2) mobile telephony and (3) internet communications. The main difference between the AmCPC and AmLOIA, at least when it comes to the object of surveillance, seems to be in the level of detail when it comes to the metadata which will be recorded in addition to the content of communications.

We do not identify serious shortcomings in the mentioned provisions when it comes to the foreseeability of interception of content powers. Namely, citizens who are subject to Armenian legislation can foresee with sufficient clarity which types of communication are subject to interception in accordance with the law. We turn now to the other issues relevant from the perspective of Article 15.

2.7.3.2 The authorities' access to communications

2.7.3.3 Authorization procedure

As explained above, surveillance of communications is one of the covert investigative actions regulated by the AmCPC. Hence, all general rules and requirements applicable to those actions apply to interception as well. Pursuant to Article 242(2) of the AmCPC, the secret investigative operation is carried out by the investigator's instruction based on the court's decision. Likewise, AmLOIA makes it clear that operational-intelligence measure of wiretapping can be made only under judicial supervision and with a prior court order.[61]

AmCPC does not regulate situation in which court order cannot be obtained expeditiously and hence some urgent procedure is being applied. Neverthless, this is regulated by the AmLOIA, which stipulates, by way of exception from general rule requiring court order for interception of communications, that "*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.[62] 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 Prime Minister of the Republic of Armenia on each case laid down in this part".*[63]

In general, we consider that the abovementioned procedures provide sufficient safeguards against arbitrary application. Most importantly, it seems that in ordinary criminal investigations it would not be possible for the law enforcement authorities to rely on the urgent authorization procedures, since that seems applicable only where terrorism or national security risks arise.

[61] AmLOIA, Articles 32(1), 34(1).
[62] AmLOIA, Article 32(2).
[63] AmLOIA, Article 32(3).

But even if this would not be the case, the fact remains that subsequent judicial authorization would be required. And if such subsequent authorization is not granted, interception must be terminated, and all information and materials destroyed immediately.

Authorizing authority's scope of review

As explained above, Armenian legislation already implements important safeguard, in that surveillance orders are issues by the courts. Next, we look at the authorization authority's scope of review. As explained in the introduction, the ECtHR has held that this authority 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 purpose of this is to ensure that "*secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration*".[64]

Regarding these conditions, we note that Article 242(1) of the AmCPC stipulates that "an undercover investigative action may be performed only when there are sufficient grounds to assume that it may result in obtaining evidence of significance to the proceedings in question, and, at the same time, obtaining such evidence in other ways is reasonably impossible". Also, regarding the reasonable suspicion, that seems to be covered by Article 243(2) of the AmCPC, which defines categories of persons against whom surveillance of communications may be applied. Hence, it appears that (compared to situation in 2018) both of the abovementioned requirements are now present in the Armenian legislation. Provided that these requirements are implemented properly by Armenian courts, in the sense that courts are undertaking genuine and serious analysis of the necessity test, it will provide adequate protection against arbitrary application.

AmLOIA implements broadly the same requirements, only using somewhat different language. Pursuant to its Article 31(4), "the operative-investigative measures provided for in clauses 8, 11, 12 and 15 of part 1 of Article 14 of this law can be conducted only in cases when the person against whom they are to be conducted, is suspected of committing a serious and particularly serious crime, and if there is solid evidence that it is impossible to obtain the information necessary for the implementation of the tasks assigned to it by this law by the body conducting the operative-investigative measure in another way".

To summarize this part up, we consider that Armenian legislation implements necessary safeguards in the domain of authorizing body's scope of review.

Precision of interception order

ECtHR has also 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".[65]

In this context, we note that the AmCPC requires that the motion of the investigator for performing communications surveillance in line with Article 241(1)(4) must indicate "the respective telephone number, e-mail address, words or word combinations of interest for the search, or other relevant personal identification data". On the contrary, we did not identify provisions in the AmCPC which would regulate in detail the content of the court's authorization

[64] Zakharov v Russia, ECtHR app. no. 47143/06, para 257.
[65] Zakharov v. Russia, para 264 and other cases quoted there.

for interception of communications. Neither were we 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.

2.7.3.4 Scope of application

As explained in the introduction of this report, it is one of the standards of the European human rights law, both under the Convention and the ECtHR's case-law, that domestic legislation must restrict the application of interception measures to a limited range of serious criminal offences. Moreover, it is also required that domestic legislation defines with precision categories of people liable to have their communications intercepted.

Compared to the situation in 2018, first of these conditions (limitation vis-à-vis categories of crimes) is now present in the Armenian legislation. AmCPC defines in Article 242(3) that "undercover investigative actions may be performed in the proceedings related to the alleged grave and particularly grave crimes as well as in the proceedings of taking and giving a bribe". Likewise, AmLOIA stipulates in Article 31(4) that "the operative-investigative measures provided for in clauses 8, 11, 12 and 15 of part 1 of Article 14 of this law can be conducted only in cases when the person against whom they are to be conducted, is suspected of committing a serious and particularly serious crime". Hence, the only difference here appears to be that AmCPC, unlike AmLOIA, also includes taking and receiving of a bribe into a list of serious offences for which interception can be ordered. This is something to be addressed in the future since there should be no ambiguity when it comes to the application of serious covert investigative powers such as interception of communications.

When it comes to scope of application of interception in relation to persons concerned, AmCPC stipulates in Article 243(2) that it can be performed:

1. In relation to the natural person concerning whom there are facts indicating the commission of the alleged crime; or

2. In relation to the Accused; or

3. In relation to the natural person concerning whom there is a grounded assumption that he has been in regular direct communication with the Accused or may reasonably communicate with him;

4. In relation to a legal person, concerning which there is a grounded assumption that its activities fully or in a relevant part are managed, controlled, or otherwise de facto directed by the persons specified in points 1 or 2.

On the other hand, AmLOIA stipulates in Article 31(4) that measure is applicable in relation to person who is suspected of committing a serious and particularly serious crime. We believe that correct application of these powers is made by giving preference to the provisions of the AmCPC, which should be seen as *lex specialis* here. Consequently, we conclude that Armenian legislation limits, in a foreseeable manner, categories of people liable to have their communications intercepted. Nevertheless, Armenian legislator might consider taking note of these discrepancies and ensuring that the AmCPC and the AmLOIA are fully in line with each other.

It also needs to be noted that some communications are legally privileged and are exempted from interception. Pursuant to Article 243(7) of the AmCPC, "it shall be prohibited to perform the undercover investigative actions envisaged by Clauses 1 to 4 of Paragraph 1 of Article 241 of this Code, if the person in relation to whom such action is to be performed communicates with his Attorney. In any event, information obtained in a result of monitoring such communication shall be destroyed immediately". Substantially the same provisions are found in Article 31(7) of the AmLOIA as well. This also represents an important safeguard.

2.7.3.5 The duration of interception

According to Article 243(5) of the AmCPC, duration of surveillance of communications is limited to a maximum of 12 months, with additional requirement that every individual court warrant is granted for a timeframe not exceeding 3 months.

In the same context, AmLOIA stipulates in its article 39(2) that surveillance of communications cannot last more than 12 months, without mentioning the requirement for individual orders not to exceed a period of 3 months. As above, since the provisions of the AmCPC and the AmLOIA are not contradicting each other here this is not serious issue. Nevertheless, Armenian legislator might consider taking note of this and further harmonizing provisions of these two statutes. Other than that, we consider that rules on duration of interception in the 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.

2.7.3.6 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. 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. 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.*

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.

2.7.3.7 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.*

2.7.3.8 Supervision and oversight

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.[66] 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.

It is very well established in the case-law of the ECtHR that due to the fact that surveillance of communications is exercised in secret, the risks of arbitrariness are evident.[67] It is therefore necessary that the state implements adequate safeguards against arbitrary application and abuse of the law. As explained by the ECtHR, "the overarching requirement is that a secret surveillance system must contain effective guarantees – especially review and oversight arrangements – which protect against the inherent risk of abuse and which keep the interference

[66] AmLOIA, Article 33.
[67] Zakharov v. Russia, paragraph 229.

which such a system entails with the rights protected by Article 8 of the Convention to what is "necessary in a democratic society"".[68]

It appears appropriate to differentiate here between supervision in specific cases, described in the sections above, and systematic oversight of the operation of secret surveillance system as such.

In this context, the ECtHR has explained that the relevant factors for deciding whether the oversight arrangements are adequate are (a) the independence of the supervisory authorities, their competences, and their powers (both to access materials and to redress breaches, in particular order the destruction of surveillance materials), and (b) the possibility of effective public scrutiny of those authorities' work.[69]

The starting element here is that it appears that in Armenia, like in many other countries, relevant authorities have direct access to networks of communication service providers and are in the position to execute surveillance without further technical or legal participation of those providers (see more extensively 7.7.1 above). In such circumstances, it is important to consider also the oversight of system as a whole.

Unfortunately, we have been able to identify only a limited number of provisions in the Armenian legislation relevant for this issue. It is prescribed in Article 27 of the AmLSSB that

> *The prime minister exercises control over the activities of the national security bodies within the framework of the powers assigned to him by the Constitution and the law.*
>
> *The deputies of the National Assembly of the Republic of Armenia have the right to receive information about the activities of the national security bodies in connection with the implementation of their parliamentary activities, in accordance with the procedure established by the legislation of the Republic of Armenia.*

We have not been able to identify other provisions relevant to this issue. But, it seems that the power of parliamentary control is severely limited at best, and includes only access to information. In such circumstances, it seems reasonable to conclude that oversight mechanisms are not in line with the relevant standards.

2.8 Summary and recommendations

- Procedural powers in Armenian legislation are regulated by the AmCPC on one side and the AmLOIA, on the other. Analysis of these documents indicates that it is not precisely clear in which cases results of evidence obtained on the basis of powers defined in the AmLOIA can be used as evidence in criminal proceedings. Hence, national authorities might consider this issue and seek to ensure that there is no ambiguity regarding the scope of application of these laws and the use of materials obtained on the basis of AmLOIA as evidence in criminal proceedings.

[68] Ekimdzhiev and Others v. Bulgaria, paragraph 292.
[69] Ekimdzhiev and Others v. Bulgaria, paragraph 292 et seq.

- AmCPC prescribes reasonably foreseeably that electronic evidence can be used in criminal proceedings.
- Armenian legislation still does not differentiate sufficiently between categories of data which form the basis for differentiation of procedural powers, namely computer data in general, subscriber information, traffic data and content data. By introducing these concepts and building on them Armenian legislation would come much closer to regulating procedural powers in line with the Convention and specifically its article 15.
- Armenian legislation still does not regulate expedited preservation of stored computer data and preservation and partial disclosure of traffic data, in line with Articles 16 and 17 of the Convention, respectively. This seriously limits the ability of Armenian authorities to apply the principle of proportionality in line with requirements of Convention's Article 15. Hence, it is recommended that the AmCPC be amended by introducing these powers.
- Production order (Article 18 of the Convention) is only partially implemented in the Armenian legislation. While there are no rules in the AmCPC regarding production of computer data in general, there are some provisions which regulate production of data which can fall within the notion of subscriber information. But the corresponding procedural power in the AmCPC also goes beyond subscriber information as they are defined in the Convention since it also includes location data (although, with appropriate safeguards). Overall, national authorities might reconsider this approach and opt for defining procedural powers in line with the Convention.
- New Armenian CPC contains new rules which correspond to the ones in Convention's Article 19, in the chapter about "digital search". It appears that this Chapter uses most important procedural safeguards, namely court authorization. There are also multiple formal requirements, which are applicable to all investigative powers, and so this one as well. There is some room for improvement regarding possible implementation of extended search (Article 19(2)) of the Convention, and rules on seizure of stored computer data (Article 19(3)) of the Convention.
- Armenian CPC treats real-time collection of traffic data under the same set of rules as content data. Regarding content data, the new AmCPC improved situation compared to the legislation which was applicable during the last assessment. Still, Armenian law does not implement all the necessary safeguards. Likewise, we have not been able to identify appropriate rules on the oversight of secret surveillance systems.

3 Azerbaijan

3.1 Relevant legal framework

This part of the Report is based on the analysis of the following statutory law of Azerbaijan:

1. Code of Criminal Procedure of the Azerbaijan Republic (hereinafter: AzCPC)[70]
2. Law on Operational-Search Activity of the Azerbaijan Republic (hereinafter: AzLOSA)[71]

Azerbaijan's Criminal Procedure Code (AzCPC) was amended multiple times since the earlier version of this report (2018). For the preparation of this document, we relied on its current publicly available consolidated version. Likewise, the Law on Operational-Search Activity (AzLOSA), originally enacted in 2002, was last amended in 2023.

The purpose of this report is overall analysis of national legislation in the implementation of procedural powers of the Convention (Articles 16 to 21), from the perspective of conditions and safeguards used to ensure protection of fundamental human rights and freedoms (Convention's Article 15). And since the procedural powers in the Convention are used to collect evidence for the purpose of specific criminal investigations or proceedings (Article 14), the primary relevant sources of regulation in the domestic law are codes on criminal procedure. But, there are many secondary issues which can be regulated by other laws as well, and hence we attempted to pursue a broader approach and also look into those sources. Nevertheless, the analysis made here is limited to conditions and safeguards applicable to actions undertaken broadly in the context of criminal proceedings. Use of procedural powers for national security, intelligence and other purposes was not analysed.

3.2 General considerations

3.2.1 Applicable national legislation

Like in other jurisdictions analysed in this report, law of Azerbaijan also regulates procedural powers relevant from the perspective of the Convention in statutes covering criminal procedure (AzCPC) and operational-search activity (AzLOSA). It is noted that the aims of the later go beyond investigations and prosecutions of specific criminal offences and include generally protecting human life, health, rights and freedoms, legal interests of legal entities, state secrets, as well as national security from criminal intent.[72] Specific tasks of the operational-search activities include prevention and detection of crimes; identification of persons who prepared, committed or committed crimes; searching for persons who are hiding from judicial, investigative and investigative bodies, who refuse to serve punishment or who are missing; and identification of unknown corpses.[73]

In terms of procedural powers, it is to be noted that AZLOSA also has powers which interfere with rights protected under Article 8 of the ECHR, including tapping telephone conversations, examination of postal, telegraphic and other correspondence and retrieving of information from

[70] Available at https://e-qanun.az/framework/46950
[71] Available at https://e-qanun.az/framework/2938
[72] AzLOSA Article 1.
[73] AzLOSA Article 1(III).

technical channels and other technical means.[74] AzLOSA is not without safeguards in this context, since it explicitly calls for judicial authorization (including special procedure for urgent authorization).[75] But there are also many shortcomings here. Most importantly, AzLOSA does not implement necessity requirement. It appears that such requirement was present in the earlier versions of the AzLOSA (until 2016) and it prescribed specifically that judge can authorized such measure "if the goals stipulated in Article 1 of this Law cannot be achieved in any other way". Nevertheless, there is no such requirement in the current version of the law, which is a serious shortcoming. Likewise, it does not appear that measures under the AzLOSA are adequately limited in duration, in relation to categories of persons subject to them, offences which might trigger their application, and so on.

Turning to the relationship between the AzCPC and the AzLOSA, we note that Article 16 of the later law stipulates that "materials obtained as a result of operative search activity according to the present Law and submitted and examined in conformity with the requirements of the Criminal Procedure Code of the Republic of Azerbaijan shall be admitted as evidence in criminal proceedings". Hence it follows that the rules of the AmCPC are relevant for the issue of recognition of evidence.

In the context of the AzCPC, it is prescribed that "the materials obtained as a result of operational-search activity can be accepted as evidence for criminal prosecution when they are obtained in accordance with the Law of the Republic of Azerbaijan "On Operational-search Activity" and are presented and checked in accordance with the requirements of this Code".[76] Moreover, "information, documents and other items obtained as a result of intelligence and counter-intelligence activities can be accepted as evidence for criminal prosecution if they are obtained in accordance with the Law of the Republic of Azerbaijan "On Operation-search Activity" and are presented and checked in accordance with the requirements of this Code".[77] But, it is not precisely clear from the legislation what does it mean that the document is "presented and checked in accordance" with the AzCPC. National authorities of Azerbaijan might want to consider this issue and ensure that national law regulates this issue with sufficient foreseeability.

3.2.2 Status of electronic evidence

AmCPC stipulates in Article 124.2.5. that evidence includes "other documents", which are defined in Article 135.1 as "paper, electronic or other carriers that contain information in the form of letters, numbers, graphics and other signs that may be important for criminal prosecution". Hence, it is regulated in a reasonably foreseeable way that electronic evidence is generally admissible under the AzCPC.

3.2.3 Categories of computer data recognized in the legislation

AzCPC does not differentiate properly between various categories of computer data. Legislation does not appear to define the notions of traffic data, subscriber information and content data.

3.3 Expedited preservation of stored computer data

[74] AzLOSA Article 10(I)
[75] AzLOSA Article 10(III)
[76] AzCPC Article 137.
[77] AzCPC Article 137-1.1.

Situation regarding expedited preservation of stored computer data in Azerbaijan remains unchanged. AzCPC still does not implement expedited preservation of stored computer data (Article 16 of the Convention) as a standalone measure. In such circumstances, law enforcement authorities of Azerbaijan can rely only on powers enumerated in Article 143 of the AzCPC, dealing with collection of evidence. More specifically, paragraph 2 of Article 143 seems to be relevant here. As will be explained below (section 3.4), Article 143.2 is, in terms of the Convention, effectively a production order. And while it is in theory possible and permissible to give effect to Article 16 by means of a production order, such approach nowadays nevertheless falls short of best comparative practices in the implementation of the Convention. Hence, it is recommended that national authorities of Azerbaijan consider amending AzCPC to ensure implementation of Convention's Article 16 as a specific and standalone procedural power, for the following reasons:

- It would enable law enforcement authorities to choose between different procedural powers and to use the one which is the most appropriate in the circumstances, which is one of the aims of the Convention.
- Above approach would contribute to the principle of proportionality, which is explicitly provided in the Article 15 of the Convention.
- It would enable national law enforcement authorities to better participate in international data exchanges in line with the Convention.
- It would enable business entities to cooperate with law enforcement authorities on the basis of clear legal framework, which would be more in line with personal data protection principles.

3.4 Expedited preservation and partial disclosure of traffic data

Situation with preservation of traffic data is similar as above (3.2). We did not identify any specific provision covering preservation and partial disclosure of traffic data (Article 17 of the Convention) in the legislation of Azerbaijan. According to explanations given by national authorities in 2018, 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.

3.5 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, this provisions seems rather general, and we did not identify and corresponding safeguards.

3.6 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.[78] 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*".[79] Moreover, "objects and documents which may be of significance as evidence may be impounded by the investigator".

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 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.[80] In certain, highly limited circumstances, it is possible to conduct a search without the court order.[81] Nevertheless, it seems that rules regarding subsequent judicial control of a search conducted without court authorization are absent from the AzCPC.

[78] Chapter XXX of the AzCPC.
[79] AzCPC, Article 242(1).
[80] AzCPC, Article 243(1).
[81] AzCPC, Article 243(3).

Next, there are precise rules regulating the contents of a search warrant,[82] participation of circumstantial witnesses, defense counsel, interpreter, experts and other persons.[83]

Finally, AzCPC contains detailed rules governing the execution of search and seizure and recording of it.[84]

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.

3.7 Surveillance of communications

3.7.1 Duties of service providers to assist in the surveillance of communications

Pursuant to Article 39 of the AzLOSA;

> *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.

3.7.2 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

[82] AzCPC, Article 243(2).
[83] AzCPC, Article 244.
[84] AzCPC, Article 245-247.

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 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.[85] 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 AZLOSA. 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.

3.7.3 Interception of content data

3.7.3.1 Legal basis

Interception of content data is, in the Azeri legislation, regulated by the AzCPC and the AzLOSA. 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 AzLOSA 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;*

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

We consider that Article 259 of the AzCPC and some parts of Article 10 of the AzLOSA 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 AzLOSA, while "tapping of telephone conversations", and "examination of postal and telegraphic 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 AzLOSA 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 AzLOSA is not necessarily linked. AzLOSA 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 AzLOSA, 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.[86] Similar solution can be found in Article 7(3) of the Georgian Law on Operative Investigatory Activities.[87]

3.7.3.2 The authorities' access to communications

Pursuant to Article 39 of the AzLOSA;

> *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

[86] See chapter 6.7.1 below.
[87] See chapter 5.7.1 below.

arbitrariness and abuse are adequately implemented. The effectiveness of those safeguards will be analysed below.

3.7.3.3 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 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".*[88]

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.[89]

Similarly, pursuant to Article 10(4) of the AzLOSA, "*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

[88] AzCPC, Article 177(4)4.
[89] AzCPC, Article 443(2)1-2.

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 legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means*".[90] The purpose of this is to ensure that "*secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration*".[91]

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 AzLOSA. 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 AzLOSA adequately implement the requirement of "necessity".

3.7.3.4 Scope of application

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

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 AzLOSA 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 and Article 10(IV) of the AzLOSA, 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.[92] This provision is sufficiently precise and foreseeable. On the other hand, pursuant to Article 11(IV) of the AzLOSA, "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".[93]

[92] AzCPC, Article 259(1).
[93] Zakharov v Russia, para 248.

3.7.3.5 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".[94]

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 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 AzLOSA 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 AzLOSA, detective-search measures can be applied for undefined time (that is, until the aim of the interception is achieved). The fact that AzLOSA 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.

3.7.3.6 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.[95] 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 AzLOSA 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 AzLOSA 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 AzLOSA 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,

[94] Zakharov, para 250.
[95] Zakharov, para 253-256.

Article 19(1) calls for judicial supervision of the detective-search activities, in accordance with the AzCPC. Thirdly, AzLOSA 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 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 AzLOSA 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.*

3.7.3.7 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.

3.7.3.8 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*".

3.7.3.9 Oversight

It is very well established in the case-law of the ECtHR that due to the fact that surveillance of communications is exercised in secret, the risks of arbitrariness are evident.[96] It is therefore necessary that the state implements adequate safeguards against arbitrary application and abuse of the law. As explained by the ECtHR, "the overarching requirement is that a secret surveillance system must contain effective guarantees – especially review and oversight arrangements – which protect against the inherent risk of abuse and which keep the interference which such a system entails with the rights protected by Article 8 of the Convention to what is "necessary in a democratic society"".[97]

It appears appropriate to differentiate here between supervision in specific cases, described in the sections above, and systematic oversight of the operation of secret surveillance system as such.

In this context, the ECtHR has explained that the relevant factors for deciding whether the oversight arrangements are adequate are (a) the independence of the supervisory authorities, their competences, and their powers (both to access materials and to redress breaches, in particular order the destruction of surveillance materials), and (b) the possibility of effective public scrutiny of those authorities' work.[98]

The starting element here is that it appears that in Azerbaijan, like in many other countries, relevant authorities have direct access to networks of communication service providers and are in the position to execute surveillance without further technical or legal participation of those providers. In such circumstances, it is important to consider also the oversight of system as a whole.

Unfortunately, we have not been able to identify provisions of national law on oversight which would be in line with the relevant European standards.

[96] Zakharov v. Russia, paragraph 229.
[97] Ekimdzhiev and Others v. Bulgaria, paragraph 292.
[98] Ekimdzhiev and Others v. Bulgaria, paragraph 292 et seq.

3.8 Summary and recommendations

- Procedural powers in the legislation of Azerbaijan are regulated by the AzCPC on one side and the AzLOSA, on the other. Analysis of these documents indicates that it is not precisely clear in which cases results of evidence obtained on the basis of powers defined in the AzLOSA can be used as evidence in criminal proceedings. Also, it appears that the AzLOSA does not implement all necessary safeguards in relation to powers which interfere with private life of individuals. Hence, national authorities might consider this issue and seek to ensure that there is no ambiguity regarding the scope of application of these laws and the use of materials obtained on the basis of AzLOSA as evidence in criminal proceedings. Also, conditions and safeguards for human right protection in the AzLOSA should be reviewed.
- AzCPC prescribes reasonably foreseeably that electronic evidence can be used in criminal proceedings.
- AzCPC still does not differentiate sufficiently between categories of data which form the basis for differentiation of procedural powers, namely computer data in general, subscriber information, traffic data and content data. By introducing these concepts and building on them legislation of Azerbaijan would come much closer to regulating procedural powers in line with the Convention and specifically its article 15.
- Legislation of Azerbaijan does not regulate expedited preservation of stored computer data and preservation and partial disclosure of traffic data in line with Articles 16 and 17 of the Convention, respectively. This seriously limits the ability of domestic authorities to apply the principle of proportionality in line with requirements of Convention's Article 15 and deprives national authorities and business entities of the possibility to exchanging data in line with personal data protection standards. Hence, it is recommended that the AzCPC be amended by introducing these powers as specific and standalone orders issued to data holders.
- Production order seems to be given effect via very general provisions which stipulates that, investigator, prosecutor, or court, at the request of the parties to the criminal proceedings, or on their own initiative, have the right to request from physical, legal and official persons to submit documents and items important for criminal prosecution. On the other hand, we did not identify any corresponding safeguards in relation to this power.
- Search and seizure is covered by general rules on search and seizure of documents. There is no implementation of specific powers defined in Articles 19(2) and 19(3) of the Convention. Some safeguards should also be improved.
- There are significant shortcomings in the implementation of Articles 20 and 21 of the Convention, and especially in corresponding safeguards. National authorities of Azerbaijan might consider making a comprehensive analysis of all national legislation pertaining to secret surveillance of communications and introducing all necessary safeguards developed in the case-law of the ECtHR. This should also include the analysis and reform of the system of oversight over the operation of secret surveillance measures in general.

4 Belarus

4.1 Relevant legal framework

This part of the report is based on the analysis of the following statutory law:

1. Criminal Procedure Code of Belarus (hereinafter: ByCPC).[99]
2. Law on operational-search activity (hereinafter: ByLOSA)

ByCPC was amended multiple times following the last report, most recently in 2023. Unfortunately, unlike other countries analysed in this report, there appears to be no fully open portal to all national legislation. Some legislation (like ByCPC) is freely available in consolidated version online, but many other laws are not easily accessible. In such circumstances, we relied on publicly available sources, including:

- the *Compedium of security sector legislation: Belarus*, which is a collection of translated national laws, available online, published in 2021.[100]
- Texts available at https://cis-legislation.com/

The purpose of this report is overall analysis of national legislation in the implementation of procedural powers of the Convention (Articles 16 to 21), from the perspective of conditions and safeguards used to ensure protection of fundamental human rights and freedoms (Convention's Article 15). And since the procedural powers in the Convention are used to collect evidence for the purpose of specific criminal investigations or proceedings (Article 14), the primary relevant sources of regulation in the domestic law are codes on criminal procedure. But, there are many secondary issues which can be regulated by other laws as well, and hence we attempted to pursue a broader approach and also look into those sources. Nevertheless, the analysis made here is limited to conditions and safeguards applicable to actions undertaken broadly in the context of criminal proceedings. Use of procedural powers for national security, intelligence and other purposes was not analysed.

4.2 General considerations

4.2.1 Applicable national legislation

In Belarus, procedural powers relevant form the perspective of the Convention are found in the ByCPC and the ByLOSA. ByLOSA, like other similar laws, pursues a very broad mandate, which goes beyond investigations and prosecutions of criminal offences.[101] Likewise, there is a broad

[99] Available at https://etalonline.by/document/?regnum=HK9900295

[100] https://www.dcaf.ch/sites/default/files/publications/documents/CompendiumLegislationBelarusCACDS_DCAF_BYC.pdf

[101] ByLOSA Article 3 prescribes the following:

Article 3. Tasks of Operational Intelligence Activities

The tasks of operational intelligence activities are:

- collecting information about events and actions that threaten the national security of the Republic of Belarus;
- preventing revealing and suppressing crimes, as well as identifying citizens who are preparing, committing or have committed crimes;

list of national agencies which can rely on powers from the ByLOSA, including Internal affairs bodies, State security Bodies, The Border Service, The Presidential Security Service, The Operational and Analytical Centre under the President of the Republic of Belarus, Financial investigation bodies of the State Control Committee, Customs authorities, The Intelligence Service of the Armed Forces of the Republic of Belarus.

In terms of procedural powers, it is to be noted that ByLOSA also has powers which interfere with rights protected under Article 8 of the ECHR, including surveillance in telecommunication networks.[102] Analysis of the ByLOSA shows multiple deficiencies which make it incompatible with the European standards. Most importantly, there seems to be no independent authority in charge of authorisation,[103] legal grounds for such activities appear to be very broad and vague,[104] there seems to be no requirement for testing the necessity and proportionality of the measure, and so on. In such circumstances, national authorities of Belarus might want to consider undertaking comprehensive reform of the national legislation, to bring it in line with the relevant standards established by the ECtHR.

4.2.2 Status of electronic evidence

Article 88(2) of the ByCPC prescribes that "sources of evidence are the testimony of the suspect, the accused, the victim, the witness, including their audio and video recording; expert opinion; evidence; protocols of investigative actions, audio or video recordings of the course of court sessions, protocols of court sessions, materials of operational-search activities, other documents and other information carriers received in the manner prescribed by this Code". Pursuant to Article 100 of the ByCPC, "other information carriers include photographic and filming materials, sound and video recordings and other information carriers received, requested or submitted in the manner prescribed by Article 103 of this Code". It is reasonably clear that electronic evidence may fall within this category.

4.2.3 Categories of computer data recognized in the legislation

ByCPC does not differentiate properly between various categories of computer data. Legislation does not appear to define the notions of traffic data, subscriber information and content data.

4.3 Expedited preservation of stored computer data

- searching for those accused of crimes who have escaped from the criminal prosecution body or court and/ or whose whereabouts are unknown to these authorities, for missing citizens, and for those sentenced to punishment in the cases established by legislative acts;
- establishing personal data for citizens who have died;
- establishing personal data for citizens who cannot report such data themselves because of their health or age;
- establishing property that is or may be subject to being seized in criminal proceedings;
- ensuring the security of citizens who provide assistance on a confidential basis to agencies performing operational intelligence activities, and their relatives, as well as the safety of their property from criminal encroachments, and ensuring the safety of other citizens in accordance with the legislation;
- collecting information for decision-making on the admission of citizens to state secrets, technical operation of facilities, threats to the life or health of citizens or the environment, participation in investigative activities, and assistance on a confidential basis to agencies performing operational intelligence activities;
- protecting state secrets.

[102] ByLOSA Article 18.
[103] ByLOSA Article 19.
[104] ByLOSA Article 16.

There are no provisions implementing expedited preservation of stored computer data in the ByCPC in line with the Article 16 of the Convention. Hence, compared to the last assessment in 2018, the situation regarding Article 16 remains largely unchanged. National authorities of Belarus might want to consider this and amend ByCPC to implement expedited preservation of stored computer data in line with the Convention, for the following reasons:

- It would enable law enforcement authorities to choose between different procedural powers and to use the one which is the most appropriate in the circumstances, which is one of the aims of the Convention.
- Above approach would contribute to the principle of proportionality, which is explicitly provided in the Article 15 of the Convention.
- It would enable national law enforcement authorities to better participate in international data exchanges in line with the Convention.
- It would enable business entities to cooperate with law enforcement authorities on the basis of clear legal framework, which would be more in line with personal data protection principles.

4.4 Expedited preservation and partial disclosure of traffic data

We have not been able to find any provisions in the legislation of Belarus implementing expedited preservation and partial disclosure of traffic data in line with the Article 17 of the Convention. Hence, compared to the last assessment in 2018, the situation regarding Article 17 remains largely unchanged. National authorities of Belarus might want to consider this and amend ByCPC in order to implement Article 17 properly.

4.5 Production order

Production order for stored computer data is not implemented in the legislation of Belarus as a specific standalone order. Nevertheless, there seems to exist some legal basis for ordering production of computer data in Article 132(2) of the ByCPC, which reads as follows:

> *2. The criminal prosecution body, as well as the court, at the request of the parties or on their own initiative, within their competence, have the right, on the basis of the materials in their production and the criminal case, in the manner prescribed by this Code, to summon any person to conduct investigative and other procedural actions or give an opinion as an expert; to carry out inspections, searches and other investigative actions provided for by this Code; require organizations, officials and citizens, as well as bodies authorized by law to carry out operational-search activities,* ***provide information, objects and documents relevant to the criminal case****; require the production of inspections from the relevant authorities and officials. The requirement of the criminal prosecution body to provide information, documents containing a secret protected by law, in the cases provided for by legislative acts, as well as to provide information, documents containing state secrets, is sanctioned by the prosecutor.*

We did not identify any other powers in the ByCPC which would regulate production of documents, including computer data. While Article 132(2) of the ByCPC appears to create some legal ground for production orders, we did not identify any specific safeguards associated with this provision.

4.6 Search and seizure of stored computer data

In the ByCPC matters falling within Article 19 of the Convention are covered in Articles 203 *et seq* of the ByCPC, which regulate inspection. The most important rules are the following:

- The basis for conducting an inspection of the scene, the corpse, the area, the premises, the dwelling and other legal possessions, objects, documents and computer information is the availability of sufficient data to believe that in the course of these investigative actions traces of a crime and other material objects may be found, other circumstances have been clarified relevant to the criminal case.[105]

- Only those objects that may be related to the criminal case or materials are subject to seizure.[106]

- If it is impossible or inappropriate to seize an object containing computer information relevant to a criminal case or verification materials, during the inspection it may be copied (fixed) in a displayable form, including the creation of an image of a computer information carrier. When copying (fixing) computer information, conditions should be provided that exclude the possibility of its loss, procedures and methods should be used to ensure the validity of the copied (fixed) computer information. An entry is made in the protocol on the implementation of copying (fixing) of computer information.[107]

Also, there is a new Article 204[1] in the ByCPC, which reads as follows:

> *1. Inspection of computer information is carried out at the place of investigative action.*
>
> *2. Inspection of computer information, access to which is carried out by means of user authentication or which contains information about the private life of a person, information constituting a legally protected secret, or other information, the distribution and (or) provision of which is limited, is carried out only with the consent of the owner of the information and in his presence or by decision of the investigator, body of inquiry with the authorization of the prosecutor or his deputy, unless otherwise provided by part 5 of this article. In urgent cases, the examination of computer information can be carried out by order of the investigator, the body of inquiry without the sanction of the prosecutor, followed by sending him a message about the inspection within 24 hours.*
>
> *3. During the examination of computer information by the investigator, the body of inquiry may take actions provided for by the functionality of information*

[105] ByCPC Article 203.
[106] ByCPC Article 204(1).
[107] ByCPC Article 204(2).

> *systems, information resources, as well as use scientific and technical means, equipment, apparatus, devices, computer programs.*
>
> *4. The protocol of the inspection of computer information must indicate the scientific and technical means, equipment, apparatus, devices, computer programs used and describe the procedure for accessing computer information, the actions taken during the inspection and the results obtained.*
>
> *5. Inspection of computer information stored in a computer system, network or on machine media seized during the performance of procedural actions sanctioned by the prosecutor shall be carried out without the sanction of the prosecutor.*
>
> *6. A protocol is drawn up on the inspection of computer information in compliance with the requirements of Articles 193 and 194 of this Code.*

There are no specific rules on implementation of Article 19(2).

4.7 Surveillance of communications

Due to limited access to legislation, have not been able to identify specific rules in the Belarus law pertaining to organisational and technical setup of secret surveillance powers.

In terms of procedural powers, it is to be noted that ByLOSA has powers which interfere with rights protected under Article 8 of the ECHR, including surveillance in telecommunication networks.[108] To begin with, it is not precisely clear whether powers under ByLOSA include surveillance of content or also corresponding traffic data. Later would logically seem to be the case, but then it would also be necessary to stipulate it in the law with necessary precision.

Analysis of the ByLOSA shows multiple deficiencies which make it incompatible with the European standards. Most importantly, there seems to be no independent authority in charge of authorisation,[109] legal grounds for such activities appear to be very broad and vague,[110] there seems to be no requirement for testing the necessity and proportionality of the measure, and so on. In such circumstances, national authorities of Belarus might want to consider undertaking comprehensive reform of the national legislation, to bring it in line with the relevant standards established by the ECtHR.

In the ByCPC the relevant provisions seem to be Article 214, which reads as follows:

> *1. In criminal cases on grave and especially grave crimes, if there are sufficient grounds to believe that negotiations using technical means of communication and other negotiations of the suspect, the accused and other persons may contain information relevant to the case, with the sanction of the prosecutor or his deputy or by decision of the Chairman of the Investigative Committee of the Republic of Belarus, the Chairman of the State Security Committee of the Republic of Belarus or the persons acting as them, listening and recording of these negotiations are allowed.*

[108] ByLOSA Article 18.
[109] ByLOSA Article 19.
[110] ByLOSA Article 16.

2. On the need to intercept the conversations and record them, the investigator, the body of inquiry shall issue a reasoned decision, which indicates the criminal case and the grounds on which this investigative action should be carried out; last name, first name, patronymic of the persons whose conversations are subject to listening and recording and for how long; an institution entrusted with the technical implementation of listening and recording conversations.

3. The decision is sent by the investigator, the body of inquiry to the appropriate institution for execution.

4. Listening and recording of conversations in any case cannot be carried out beyond the period of preliminary investigation of the criminal case and are canceled by the decision of the investigator, the body of inquiry.

5. The investigator, the person conducting the inquiry, during the entire established period, has the right to demand a phonogram for examination and listening at any time. It is transferred to the investigator, the person conducting the inquiry, in a sealed form with a cover letter, which must indicate the start and end times of the recording of the negotiations and the necessary technical characteristics of the means used.

6. Inspection and listening to the phonogram are carried out by the investigator, the person conducting the inquiry, if necessary with the participation of a specialist, about which a protocol is drawn up in compliance with the requirements of Articles 193 and 194 of this Code, in which the part of the phonogram of the negotiations that is relevant to the criminal case must be reproduced verbatim. The phonogram is attached to the protocol, while its part, which is not related to the case, is destroyed after the end of the criminal case.

While there seem to exist some procedural safeguards here (limitation to only serious criminal offences), many others are completely missing or a insufficient. For instance, it is possible to order surveillance of communications of "other persons", in addition to the suspect or the accused. This notion is however very vague and open ended, and hence particularly prone to abuse. Also, there are no appropriate rules on duration of measure, notification requirements, obligation to destroy data in certain cases. Authorizing body is prosecutor, which is problematic in itself, and it also appears that there is no testing of necessity to apply this measure. In such cases, it must be concluded that Belarusian legislation is not in line with the relevant European standards.

4.8 Summary and recommendations

- Procedural powers which are prescribed in the ByLOSA appear not to be in line with the relevant European standards. National authorities might consider reforming this legislation to ensure that it implements the most important conditions and safeguards identified in the case-law of the ECtHR.
- ByCPC prescribes reasonably foreseeably that electronic evidence can be used in criminal proceedings.

- Legislation of Belarus still does not differentiate sufficiently between categories of data which form the basis for differentiation of procedural powers, namely computer data in general, subscriber information, traffic data and content data. By introducing these concepts and building on them national legislation would come much closer to regulating procedural powers in line with the Convention and specifically its article 15.
- Legislation of Belarus does not regulate expedited preservation of stored computer data and preservation and partial disclosure of traffic data in line with Articles 16 and 17 of the Convention, respectively. This seriously limits the ability of domestic authorities to apply the principle of proportionality in line with requirements of Convention's Article 15 and deprives national authorities and business entities of the possibility to exchanging data in line with personal data protection standards. Hence, it is recommended that the AzCPC be amended by introducing these powers as specific and standalone orders issued to data holders.
- Production order seems to be given effect via very general provisions which stipulates that relevant authorities have the right to require organizations, officials and citizens, as well as bodies authorized by law to carry out operational-search activities, to provide information, objects and documents relevant to the criminal case. On the other hand, we did not identify any corresponding safeguards in relation to this power.
- There are most important elements of Article 19 of the Convention (search and seizure of stored computer data) in the legislation of Belarus. The main issue here appears to be the fact that authorization for these measures is given by the prosecutors. In the absence of access to all relevant legislation of Belarus it is impossible to conclude whether prosecutors enjoy necessary level of independence in other to be able to be considered competent authority in line with the standards of the ECtHR.
- System of surveillance of communications appears to be regulated only marginally in the ByCPC and the ByLOSA. Both laws show many shortcomings in the implementation of relevant European standards. We did not find any provisions which would indicate the existence of appropriate oversight mechanisms.

5 Georgia

5.1 Relevant legal framework

This part of the Report is based on the analysis of the following legislation of Georgia:

1. Georgian Criminal Procedure Code (hereinafter: GeCPC)[111]
2. Georgian Law on Operative Investigatory Activities (hereinafter: GeLOIA)[112]
3. Georgian Law on Electronic Communications (hereinafter: GeLEC)[113]
4. Georgian Criminal Code (hereinafter: GeCC)[114]
5. Rules of Procedure of the Parliament of Georgia (hereinafter: RPPG).[115]

All these laws have been amended multiple times since the earlier version of this report (2018). For the preparation of this document, we relied on their publicly available consolidated versions.

The purpose of this report is overall analysis of national legislation in the implementation of procedural powers of the Convention (Articles 16 to 21), from the perspective of conditions and safeguards used to ensure protection of fundamental human rights and freedoms (Convention's Article 15). And since the procedural powers in the Convention are used to collect evidence for the purpose of specific criminal investigations or proceedings (Article 14), the primary relevant sources of regulation in the domestic law are codes on criminal procedure. But, there are many secondary issues which can be regulated by other laws as well, and hence we attempted to pursue a broader approach and also look into those sources.

5.2 General considerations

5.2.1 Applicable national legislation

Various procedural powers which can be used by law enforcement agencies are regulated in the GeCPC and also in the GeLOIA. General observations made in relation to the concept of similar laws of other countries are equally relevant here. GeLOIA pursues relatively broad aims which go beyond investigations of specific criminal offences[116]. Multiple national authorities have the right to undertake measures prescribed in this law: (1) the operational agencies and investigation units of the Ministry of Internal Affairs of Georgia; (2) the authorised units of the State Security Service of Georgia; (3) the operational agencies of the Special State Protection Service of Georgia; (4) the operational agencies and investigation units of the Ministry of Finance of Georgia; (5) the Analytical Department, the Investigation Department and the security services of the Penitentiary Department of the Ministry of Corrections of Georgia and the security services of penitentiary institutions; (6) the operative, investigative and intelligence units of the

[111] Available at https://www.matsne.gov.ge/en/document/view/90034?publication=151
[112] Available at https://matsne.gov.ge/ka/document/view/18472?publication=52
[113] Available at https://matsne.gov.ge/ka/document/view/29620?publication=45
[114] Available at https://www.matsne.gov.ge/en/document/view/16426?publication=247
[115] English translation available at http://old.parliament.ge/en/ajax/downloadFile/131641/ROP_as_of_27_Dec_2018_ENG.pdf.
[116] GeLOIA, Article 3.

Ministry of Defence of Georgia; (7) the operational agencies of the Georgian Intelligence Service; (8) the investigators of the Prosecutor's Office; (8) the investigators of the relevant units of the Ministry of Justice of Georgia and the employees of the Operations Division of the Ministry of Justice of Georgia.[117] But, there seems to be prescribed relatively clearly in the GeLOIA that covert procedural powers defined therein, when they are executed in the context of criminal proceedings, need to comply with the GeCPC as well. Hence, we do not see this duplicity of norms as a serious issue under Article 15 of the Convention.

5.2.2 Status of electronic evidence

The notion of evidence is defined in Article 3(23) of the GeCPC as follows: "information or an item, a document, substance or any other object containing the information submitted to the court in the manner prescribed by law, which parties use in a court to prove or refute certain facts and make their legal evaluation, perform duties, protect their rights and lawful interests, and which a court uses to establish whether there exists a fact or an act because of which a criminal proceeding is conducted, whether a certain person has committed a certain act and whether or not a person is guilty, also to establish circumstances that affect the nature and degree of liability of the accused, and characterise the person. A document is considered to be evidence if it contains information required for the establishment of factual and legal circumstances of a criminal case. 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".

It follows clearly from this definition that computer data can also be considered a document and hence the evidence for the purposes of the GeCPC.

5.2.3 Categories of computer data recognized in the legislation

Georgian legislation seems to rely on basic concepts and categories of computer data as they are regulated in the Convention.

Article 3 of the GeCPC gives the following definitions which are relevant from the perspective of the Convention:

- **Computer system** – any mechanism or a group of interconnected mechanisms which, through a software, automatically processes data (including a personal computer, any equipment with a microprocessor, as well as a mobile phone).
- **Computer data** – information displayed in any form convenient for processing in a computer system, including software that ensures the operation of the computer system.
- **Service provider** – any natural or legal person that provides users with an opportunity to interact through a computer system, as well as any other person that processes or stores computer data on behalf of such communication services or of the consumers of such services.
- **Internet traffic data** – any computer data related to communications and generated by a computer system that are part of a communications chain and that indicate the

[117] GeLOIA, Article 12.

source of communication, destination, direction, time, date, size, duration and type of the basic service.

Moreover, Article 136(2) of the GeCPC defines "**information about the user**" in line with the definition of "subscriber information" in Article 18 of the Convention.

Also, the notion of "**electronic communication identification data**" is defines in the GeLEC (Article 2(z[69])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". This definition is in line with the one of traffic data found in Article 1(d) of the Convention.

The existence of these definitions in Georgian legislation has several benefits. Firstly, they are largely in line with the Convention and hence bring domestic law further in line with international standards. Secondly, they enable constructions of procedural powers in line with scope, structure and purpose of those powers as they are regulated by the Convention.

Moreover, there are some definitions in the Georgian law which do not have their counterparts in the Convention, but which still contribute to the precision and foreseeability of domestic law. These include, also from Article 3 of the GeCPC:

- Retrieval and recording of information from a communication channel – the retrieval and recording by a state body with an appropriate authority of current, transmitted, received, collected, processed or accumulated information from electronic communication (electronic mail), communication network, telecommunication or information systems by using technical means and/or software tools.
- Retrieval and recording of information from a computer system – the retrieval and recording by a state body with an appropriate authority of information transmitted and received from a computer system, as well as of current, collected, processed or accumulated information in a computer system by using technical means and/or software tools.
- Real-time geolocation identification – the real-time identification of the geographical location of mobile communication equipment with a maximum possible accuracy.
- Covert eavesdropping and recording of telephone communication – the covert eavesdropping and recording of telephone communication performed through common usage electronic communication networks and means of a person authorised under the Law of Georgia on Electronic Communications.
- Technical identifier of an object of a covert investigative action – the identification data of communication equipment used by an object of a covert investigative action (any data that allow the individual identification of communication equipment, or help in its individual identification (including a telephone number, internet protocol address (IP address), International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), MAC address, etc.)), or a user name.

5.3 Expedited preservation of stored computer data

There have been no significant changes regarding the expedited preservation of stored computer data in Georgian legislation after the last report in. Georgian law still does not implement expedited preservation of stored computer data as a standalone measure. To achieve the purpose of Article 16 of the Convention, Georgian authorities continue to rely upon Article 136 of the GeCPC, which regulates the power of "requesting a document or information". In the system of procedural powers defined by the Convention this corresponds to production order.

While this is not in itself contrary to the Convention, provided that national authorities can ensure expedited production of data and hence urgent preservation of evidence, such an approach still falls short of best comparative practices. Hence, we continue to believe 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. Also, true preservation orders should be less demanding in terms of conditions and safeguards, which makes them more appropriate, especially in the context of international cooperation requests.

5.4 Expedited preservation and partial disclosure of traffic data

Power of expeditious preservation and partial disclosure of traffic data (Article 17 of the Convention on Cybercrime) is not implemented in the Georgian legislation as a standalone procedural power. In this context, we note that Georgia operates a complex data retention system, which enables its authorities to at least partially achieve the purpose of Article 17. But this does not equate to full implementation of Article 17, which is problematic for the very same reasons as mentioned above (regarding Article 16). Hence, national authorities might want to consider implementing Article 17 as a standalone measure to ensure full harmonization with the Convention.

5.5 Production order

5.5.1 Production order for computer data in general

In Georgian legislation, purpose of Convention's Article 18 is achieved through provisions in Article 136 of the GeCPC, which regulates power of "requesting a document or information". Pursuant to 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 or the defence 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". And considering the notion of "document" in the GeCPC (see section 5.2.2. above) as well as the wording of Article 136(1), there is no doubt that the power to request document

or information includes computer data. Hence, we consider that Article 136(1) of the GeCPC is sufficiently precise and foreseeable and therefore acceptable from Article 15 perspective.

In Georgian law, production order, that is "request for a document or information", is generally authorized by a court. In order to issue this order the court needs to be satisfied that 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". Only in urgent circumstances such order can be authorised by a prosecutor, which is subject to subsequent court review (Article 112(5) of the GeCPC). We consider this to be an important safeguard against abuse.

In general, we do not identify any other issues with Article 136 of the GeCPC which would be problematic from the standpoint of Article 15 of the Convention.

5.5.2 Production order for subscriber information

Production order for subscriber information is also covered by Article 136 of the GeCPC. Pursuant to second paragraph of this Article and provided that "there is a 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". This provision appears to be narrower than required by the Convention. Namely, pursuant to Article 14 of the Convention procedural powers defined in its Chapter 2, Section 2, should be applicable to collection of electronic evidence of any crime, and not just those crimes carried "through a computer system". While this is not in itself problematic from the perspective of Convention's Article 15, national authorities of Georgia might want to consider this and broaden the application of Article 136(2) so that power defined therein can be used when investigating any criminal offence.

Subject of Article 136(2) is "information about the user". Pursuant to Article 136(3), this category is defined as "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 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 we 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. It rightly covers data in both computer and tangible forms, so the whole scope of Article 18 is adequately covered.

In general, conditions and safeguards applicable to production of subscriber information are the same as for computer data in general. As noted above, we do not identify any issues which would be problematic from the standpoint of Article 15 of the Convention.

5.6 Search and seizure of stored computer data

Georgian CPC does not contain specific procedural power for searching of computer data. In such circumstances, traditional procedural powers of search and seizure serve as a legal ground also for search and seizure of computer data, but with some specificities of applying this power to computer data addressed by the GeCPC. 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, search and seizure are carried out "with the aim of discovering and removing an object, document, substance or other object containing information that is important to the case." In order to issue such an order, pursuant to Article 119(3), there must exist a reasonable assumption that the object in question is kept in a certain place, with a certain person, and a search is required to find it. Pursuant to Article 120(5) of the GeCPC, the following items can be seized:

- the subject, document, substance, or other object containing information, which is mentioned in the ruling or resolution.
- all other objects containing information that may be of evidentiary importance for this case or that clearly indicate another crime.
- objects, documents, substances or other objects containing information removed from civil circulation.

Georgian legislation seeks to limit interference into private sphere of the individuals by prescribing in Article 120(4) that the investigator executing the search shall offer "to the person with whom the seizure or search is carried out the voluntary handover of the subject, document, substance or other object containing information. In case of voluntary handover of the object to be removed, the mentioned fact is recorded in the protocol, and in case of refusal of its voluntary handover or its incomplete handover, removal is done by force".

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, 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.[118] In such circumstances, it is necessary to follow procedure stipulated in Article 112, which reads as follows:

> *5. An investigative action provided for 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,*

[118] GeCPC, Article 120(1).

or when a delay makes it impossible to obtain the above data, or when an item, a document, substance or any other object containing information that is necessary for the case has been found during the carrying out 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 carrying out the investigative action urgently. 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 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 carried out investigative action as lawful;

b) finding the carried out 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 judgment 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 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 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 and 123.

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 already in 2018, 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 the 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, a 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.

Also, it appears that the legislation does not contain rules regarding extended search (Article 19(2) of the Convention).

5.7 Surveillance of communications

5.7.1 Duties of service providers to assist in the surveillance of communications

Organizational and technical setup for surveillance of electronic communications is regulated by the GeLEC, which prescribes in Article 8^1 as follows:

> *1. The authorised body shall have the possibility to obtain real time communication and its identification data transmitted through the infrastructure of an electronic communication company using stationary or semistationary technical possibilities and for this purpose the authorised body shall:*
>
> *a) if necessary, place/install lawful interception management system and/or necessary hardware and software related to its function free of charge;*
>
> *b) require from the electronic communication company to possess technical stationary possibility to provide real time communication content and its identification data to the authorised body in accordance with the architecture and interface defined by the technical stationary possibility to obtain real time communication.*
>
> *2. After organising technical stationary and semistationary possibilities to obtain real time communication defined in paragraph one of this article, the authorised body shall carry out the measures to obtain real time communication directly, without interference of the electronic communication company and legal participation, in accordance with the procedures established by Article 1433 of the Criminal Procedure Code of Georgia and Articles 12-14 of the Law of Georgia on Counter Intelligence Activities.*
>
> *3. The architecture and interface of the technical stationary possibility to obtain real time communication shall be established by the normative acts of the authorised body.*
>
> *4. The rules for organising and carrying out the interception of the content of the communication transmitted through the electronic communication network*

> *and its identification data using technical semistationary possibility shall be established by the normative acts of the authorised body.*

Also, communication service providers are required to set-up a system for determining geolocation in real-time. This is provided by Article 8[4] of the GeLEC, which reads as follows:

> *1. The authorised body is entitled to have the possibility to obtain real time geolocation from the network and station infrastructure of the electronic communication company which provides mobile communication networks and means and/or services and place/install relevant hardware and software on the mentioned infrastructure free of charge. The authorised body shall carry out the further actions to define real time geolocation in accordance with the procedure established by Article 1433 of the Criminal Procedure Code of Georgia and Articles 12-14 of the Law of Georgia on Counter Intelligence Activities.*
>
> *2. The system for defining real time geolocation shall ensure the possibility for defining real time geolocation of the communication equipment initiating notification of Legal Entity under Public Law called Public Safety Management Center 112 operating under the governance of the Ministry of Internal Affairs of Georgia.*
>
> *3. The architecture and interface of the system for defining real time geolocation shall be established by the normative act of the authorised body.*

It follows clearly from the rules above that electronic communication service providers must support surveillance in **real time** of both the **communication content** and its **identification data**. The notion of "electronic communication identification data" is defines in the GeLEC 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". This definition is in line with the one of traffic data found in Article 1(d) of the Convention. Moreover, Georgian legislation also provides for real-time observations of users geolocation.

Notion of "identification data of communications" includes also "user identification data", which is not defined, but presumably refers to categories of data falling within the Convention's concept of subscriber information). This would also be in line with Article 136(2) of the GeCPC which defines "information about the user" in line with the definition of "subscriber information" in Article 18 of the Convention. In our opinion, the above provisions are sufficiently precise and foreseeable in the sense that citizens have adequate foreseeability regarding categories of data which are subject to secret surveillance measures.

Electronic communications service providers are required to support surveillance by:

- Allowing authorized state body to place or install necessary hardware and software for lawful interception into their communications systems

- Ensuring that they possess "technical stationary possibility" of intercepting content data and collecting traffic data in real time, pursuant to architecture (technical specifications) determined by authorized state body

System above results in the possibility for authorized state body to carry out surveillance directly, that is without technical and legal participation of the electronic communications service provider. As is emphasized by the ECtHR, such systems of surveillance are "particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great".[119]

In this context, it is important to note that Article 8^2 of the GeLEC provides that

> *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 State Inspector Service.*

This is a very important safeguard. In terms of oversight, logging of application of secret surveillance measures and making this information available to oversight bodies greatly improves the transparency of the system and reduces the risks of abuse. But, in this context we also note that Article 8^2 of the GeLEC obliges electronic communications companies to make records about application of surveillance powers effectively only about traffic data and in the context of criminal proceedings. On the other hand, logging information about executed interceptions of content data, as well as application of all of these powers in the context of intelligence and security operations, appears to be uncovered by the GeLEC. While this might be just the issue with translation or a simple inconsistency in the legislation, national authorities might nevertheless look into this issue and ensure that logging obligation is prescribed for all types of surveillance and applicable in all legal domains where surveillance is regulated.

Also, it is necessary to consider Article 8^3 of the GeLEC, which regulates copying the databases of the electronic communication identification data by the authorised body, and reads as follows:

> *1. The authorised body shall be entitled to copy the databases of the electronic communication identification data and store them at the central bank of the electronic communication identification data in accordance with the term established by Article 15(1) of the Law of Georgia on Legal Entity under Public Law called Operative and Technical Agency of Georgia.*
>
> *2. In order to copy the databases of the electronic communication identification data provided for by paragraph one of this article the authorised body shall be entitled to have an access on the relevant databases of the electronic communication company. The technical procedure for copying the databases of the electronic communication identification data shall be established by the normative acts of the authorised body.*

But, it appears at least on the basis of legislation and without being in the position to analyse this more thoroughly that if authorized state bodies have the right to copy the whole database containing communication identification data (i.e., traffic data), than procedure described in Article 8^1 appears to be of limited value, since it appears applicable only on traffic data obtained

[119] Zakharov v Russia, paragraph 270.

in real-time. Hence, corresponding safeguard of logging (Article 8^2) appears to have reduced impact. National authorities might also want to reassess these rules.

5.7.2 Real-time collection of traffic data

Technical setup for real-time collection of traffic data was elaborated above (5.7.1). Now we turn to procedural rules authorizing the application of this power.

Real-time collection of traffic data is regulated by Article 137 of the GeCPC, which defines power of law enforcement authorities to request **real-time collection of internet traffic data**. Pursuant to first paragraph of this article, "if there is a reasonable assumption that a person commits a criminal act using a computer system, the prosecutor is authorized to apply to the court, depending on the place of investigation, to issue a ruling on the ongoing collection of Internet traffic data, by which the service provider is obliged to cooperate with the investigation and assist him in the ongoing collection or recording of such Internet traffic data, which are related to specific communications carried out on the territory of Georgia and transmitted through the computer system".

Internet traffic data is defined in Article 3(30) as "any computer data related to communications and generated by a computer system, which is part of the communication chain, indicating the source, destination, direction, time, date, size, duration, type of basic service of the communication". It is obvious that this definition corresponds fully to the one of "traffic data" in the Article 1(d) of the Convention. Looking from the perspective of the quality of law, these provisions are sufficiently precise and foreseeable.

It appears that Article 137 of the GeCPC envisages the use of this power only in cases where there is suspicion that a crime was committed "using a computer system". But, pursuant to Article 14 of the Convention scope of application of procedural powers is broader and should include collection of electronic evidence of any crime. National authorities of Georgia might consider this and broaden the application of Article 137 to be fully in line with the Convention.

In terms of **conditions and safeguards**, it is particularly relevant that real-time collection of internet traffic data is per Article 137, read in conjunction with the Articles 143^2–143^{10}, defined as one of the covert investigative actions in the legal system of Georgia. Consequently, all the conditions and safeguards applicable to interception of content data are also valid here. These conditions and safeguards are analysed bellow (5.8). This ensures a very strong protection of traffic data, which also leads to high level of compliance with the Article 15 of the Convention.

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.

5.7.3 Interception of content data

5.7.3.1 Legal basis for interception of content data in domestic legislation

The legal basis in Georgian legislation for interception of content data is found in Article 138 of the GeCPC ("Obtaining of content data"). This article 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. The provisions of Articles 143^2–143^{10} shall apply to the investigative actions provided for by this article.*

This article remained unchanged following the last assessment (2018). We consider it 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 of communications are contained within one statute. This removes some of the ambiguity that exists in the legislation of some other countries analysed in this report and significantly contributes to the clarity and foreseeability of the legislation.

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 also provide for relevant conditions and safeguards.

5.7.3.2 Authorization procedure

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".[120]

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[121]
2. limitations regarding the categories of people whose communications may be intercepted have been satisfied[122]
3. "covert 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, for preventing riots or crime, for protecting the interests of a country's economic welfare or any other person's rights and freedoms"[123]
4. "as a result of the requested covert 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"[124]. In this context, prosecutor's motion must also 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."[125]

Once the motion is submitted to the judge, the following ensues:[126]

1. Judge is required to review the motion within 24 hours, with or without an oral hearing.
2. In a ruling granting authorisation the judge must provide justification for the existence of previously mentioned circumstances. Hence, contrary to solutions in some other countries, judges are required to specifically elaborate on the conditions of necessity and proportionality.
3. Decision on the motion is made in several copies and these are dispatched to relevant bodies, including to the Personal Data Protection Service, which conducts oversight. This is to be done immediately following the ruling, and in no case later than 48 hours after the ruling.
4. Interception is implemented by the Operative-Technical Agency of Georgia ('the Agency'), which is a body with an exclusive authority to carry out covert investigative actions. Agency can initiate interception only after the Personal Data Protection Service has been notified and provided with the operative part of the judge's ruling.

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). Those

[120] GeCPC, Article 143^3(1, 17).
[121] GeCPC, Article 143^3(2a).
[122] GeCPC, Article 143^3(2b).
[123] GeCPC, Article 143^3(2c).
[124] GeCPC, Article 143^3(2d).
[125] GeCPC, Article 143^3(3).
[126] GeCPC, Article 143^3(5-5^6).

provisions also do not seem problematic from the perspective of Article 15 because relevant safeguards are implemented, most importantly:

1) There is a subsequent judicial control (in no later than 48 hours)

2) Judge has the right to review collected material before deciding on the legality of interception initiated by the prosecutor's order

3) Personal Data Protection Service is also properly notified of all undertaken measures.

Another very important safeguard is contained in Article143^3(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.*

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.

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".[127]

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.*[128]

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, 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.[129] 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.

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*

[127] Zakharov v. Russia, para 260 and other cases quoted there.
[128] Article $143^2(2)(b)$
[129] Article $143^2(10)$

> *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.

5.7.3.3 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.

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 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 also sufficiently precise and otherwise 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.

5.7.3.4 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*".[130]

GeCPC regulates the duration of interception in much detail. These provisions have been substantially amended after the last assessment, and now read as follows (Article 143^3):

> *12. A covert investigative action shall be carried out for a period specified in a ruling of a judge. This period shall correspond to the duration that is required to achieve the goal of the investigation.*
>
> *12^1. Covert investigative actions may be carried out in three stages, except in the case provided for by paragraph 12^7 of this article. At the first stage, covert investigative actions shall be carried out for not more than 90 days based on the ruling of a judge rendered upon a prosecutor's reasoned motion; at the second stage, covert investigative actions shall be carried out for not more than 90 days based on the ruling of a judge rendered upon a superior prosecutor's reasoned motion; and, at the third stage, covert investigative actions shall be carried out for not more than 90 days based on the ruling of a judge rendered upon a reasoned motion of the General Prosecutor of Georgia or his/her deputy.*
>
> *12^2. If the respective goal has not been achieved at the first stage of carrying out covert investigative actions, and if the time limit determined for the first stage of carrying out covert investigative actions has not expired, a prosecutor shall have the right to file a motion with a court requesting the extension of the time limit for carrying out covert investigative actions for the remaining period.*
>
> *12^3. If the 90-day time limit determined for the first stage of carrying out covert investigative actions has expired but the respective goal has not been*

[130] Zakharov v Russia, para 250.

achieved, the time limit for carrying out covert investigative actions may be extended, based on a ruling of a judge rendered upon a superior prosecutor's reasoned motion, for not more than the period determined for the second stage of carrying out covert investigative actions, which is 90 days.

12[4]. If the respective goal has not been achieved at the second stage of carrying out covert investigative actions, and if the time limit determined for the second stage of carrying out covert investigative actions has not expired, a superior prosecutor shall have the right to file a motion with a court requesting the extension of the time limit for carrying out covert investigative actions for the remaining period.

12[5]. If the 90-day time limit determined for the second stage of carrying out covert investigative actions has expired but the respective goal has not been achieved, the time limit for carrying out covert investigative actions may be extended, based on a ruling of a judge rendered upon a reasoned motion of the General Prosecutor of Georgia or his/her deputy, for not more than the period determined for the third stage of carrying out covert investigative actions, which is 90 days.

12[6]. If the respective goal has not been achieved at the third stage of carrying out covert investigative actions, and if the time limit determined for the third stage of carrying out covert investigative actions has not expired, the General Prosecutor of Georgia or his/her deputy shall have the right to file a motion with a court requesting the extension of the time limit for carrying out covert investigative actions for the remaining period. The time limit for carrying out covert investigative actions shall not be further extended, except in the case provided for by paragraph 127 of this article.

12[7]. If the 90-day time limit determined for the third stage of carrying out covert investigative actions has expired but the respective goal has not been achieved, based on a ruling of a judge rendered upon a reasoned motion of the General Prosecutor of Georgia or his/her deputy:

a) the time limit for carrying out covert investigative actions may be extended again for not more than 90 days if the covert investigative actions are being carried out based on a court ruling rendered in the case provided for by the Law of Georgia on International Cooperation in Criminal Matters. If the respective goal has not been achieved at this stage of carrying out covert investigative actions, and if the time limit determined for this stage of carrying out covert investigative actions has not expired, the General Prosecutor of Georgia or his/her deputy shall have the right to file a motion with a court requesting the extension of the time limit for carrying out covert investigative actions for the remaining period. The time limit for carrying out covert investigative actions shall not be further extended;

b) the time limit for carrying out covert investigative actions may be extended as many times as there are appropriate legal grounds determined by this Chapter, that are necessary for carrying out covert investigative actions, if the investigation is being carried out in relation to crimes provided for by Articles 108, 109, 143-143[2], 144-144[3], 223-224[1], 230−232, 234-235[1], 255[1], 260(4)-(7), 261(4)-(8), 262 and 263, and Chapters XXXVII−XXXVIII and XLVII, of the

> *Criminal Code of Georgia. In this case, the time limit for carrying out covert investigative actions may be extended for not more than 90 days each time.*
>
> *12[8]. A motion requesting the extension of the time limit for carrying out covert investigative actions under paragraphs 121−127 of this article shall, in addition to the circumstances provided for by paragraph 2 of this article, include information on the data obtained as a result of the commenced covert investigative actions, and specify the reasons due to which the data sufficient for investigation could not have been obtained. When rendering a ruling under paragraphs 121−127 of this article, a judge shall take into consideration an appropriate legal ground determined by this Chapter, that is necessary for carrying out covert investigative actions.*
>
> *12[9]. If covert investigative actions have been terminated, after which any legal ground necessary for carrying out covert investigative actions has emerged, the covert investigative actions shall be resumed from the stage at which they have been terminated. The covert investigative actions shall be resumed in accordance with the procedure established by this Chapter.*

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.

One new solution of Georgian legislation since the last assessment is the provision in the abovementioned paragraph 12[7](b), which provides for a possibility of unlimited renewals of interception orders for a limited number of offences. These include broadly murder; unlawful imprisonment; human and child trafficking; hostage taking; torture (including threat thereof); humiliation or inhuman treatment; creation of management of illegal formations and criminal enterprises; banditry; various offences pertaining to misuse nuclear material; transit or import of radioactive, toxic, industrial or household waste and similar offences; engagement of minors in illegal production and sale of pornographic works or other similar items; Illegal sale of drugs; their analogues, precursors or new psychoactive substances, and also some offences pertaining to their manufacturing, production, purchase, storage, transportation, transfer or sale. Moreover, all offences against constitutional structure and security principles of Georgia, terrorism and crimes against humanity, peace and security and against international humanitarian law are also included.

While the introduction of these new provisions goes in the direction of extending interception powers, it needs to be noted that pursuant 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 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". In that sense, new provision explained above are not in themselves problematic. This is especially so because other provisions of the GeCPC seem to implement adequate rules specifying when interception must be cancelled. In that context, Article 1436, which reads as follows, is relevant:

> *1. A decision to terminate a covert investigative action shall be made by a prosecutor upon application of an investigator, or on his/her own initiative. A prosecutor shall immediately notify a state body with an appropriate authority*

> *about the decision to terminate a covert investigative action, which will terminate the covert investigative action immediately after the decision is made.*
>
> *2. A covert investigative action shall be terminated if:*
>
> *a) a specific objective provided for by a ruling authorising a covert investigative action has been accomplished;*
>
> *b) circumstances are discovered that confirm that the specific objective provided for by the ruling on the given covert investigative action cannot be achieved due to objective reasons, or the carrying out of the covert investigative action is 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 covert investigative action.*

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 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.

5.7.3.5 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 covert investigative actions and relevant investigative authorities shall be responsible for appropriately safeguarding the information obtained as a result of covert investigative actions.*
>
> *2. A body carrying out a covert investigative action shall keep a record of the following data related to covert investigative actions: the type of a covert investigative action; the start and end time of the covert investigative action; an object of a covert investigative action; if a covert investigative action under Article 1431(1)(a-c) of this Code is carried out – a technical identifier of an object of a covert investigative action; the requisites 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 covert investigative action. The protocol shall exactly specify the legal grounds for carrying out the covert investigative action, its start and end time, the place where the protocol was drawn up, the type of the covert investigative action carried out and the technical means used for carrying it out, a place of carrying out a covert investigative action, an object of a covert investigative action, and if any of the covert investigative actions under Article 1431(1)(a-c) of this Code is carried out – also a technical identifier of an object of a covert investigative action. This protocol shall be forwarded to an appropriate authorised investigative body which shall immediately submit it to the prosecutor, the court registry of covert investigative actions and to the Personal Data Protection Service. The protocol shall also be forwarded to the defence in cases provided for and in the manner prescribed by this Chapter.*

Moreover, "When a covert investigative action is carried out, if requested by a prosecutor/judge, a body carrying out the covert investigative action shall issue an interim protocol".[131]

[131] Article 143^6(15)

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 covert 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 covert 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 covert 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 actions 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 covert investigative actions, which are recognised by a court as inadmissible evidence, shall be immediately destroyed six months after the court of final instance renders a ruling on the case. 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 covert investigative actions that are attached to a case as 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 materials before its destruction shall be responsible for adequate keeping of the materials obtained as a result of covert investigative actions.*
>
> *5. In cases provided for by paragraph 1 of this article, the information obtained as a result of covert 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/a judge of the court who/whose judge made a decision on the carrying out of this covert investigative action, or recognised as lawful/unlawful the covert 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 covert investigative actions, signed by the relevant*

> *prosecutors and judges, shall be forwarded to the Personal Data Protection Service, and shall be entered into the court registry of covert investigative actions.*
>
> *6. In cases provided for by paragraphs 2 and 3 of this article, the materials obtained as a result of covert 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 carrying out of the covert investigative action or recognised as lawful or unlawful the covert investigative action that was carried out without a court ruling in the case of urgent necessity.*

Finally, we note that Personal Data Protection Service, 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.

5.7.3.6 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],

> *1. Only investigators, prosecutors and judges may, before the completion of covert 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).*
>
> *2. The information obtained as a result of covert investigative actions shall be provided to the party according to Article 83(6), also in the case of approval of a plea bargain.*
>
> *3. A person against whom a covert investigative action has been carried out, shall be notified in writing of the carrying out 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 carrying out of covert 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 1433(15) of this Code. A decision as to the time when a person is to be notified of the carrying out of covert 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 carrying out of covert investigative actions against him/her within 12 months after*

ending/terminating the covert 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 carrying out of the covert investigative actions, and request the postponement, for no longer than 12 months, of the provision of information to the relevant person on the carrying out of the covert 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 an 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.

5. If, after the granting of a motion determined by paragraph 4 of this article and the expiration of the respective time limit, the risk determined by the same paragraph still exists, a prosecutor shall have the right to request twice the postponement of the provision of information to a relevant person on the carrying out of the covert investigative actions, in accordance with the procedure established by the same paragraph. A prosecutor shall have the right to request the postponement of the provision of such information for not more than 12 months each time.

6. If covert investigative actions have been carried out in relation to crimes provided for by Articles 108, 109, 143-1432, 144-1443, 223-2241, 230−232, 234-2351, 2551, 260(4)-(7), 261(4)-(8), 262 and 263, and Chapters XXXVII−XXXVIII and XLVII, of the Criminal Code of Georgia, the notification of the carrying out of covert investigative actions to a person, against whom the covert investigative actions have been carried out, may be postponed as many times as necessary to prevent risks to national security, public order, and the interests of legal proceedings. In this case, the notification of the carrying out of covert investigative actions to a relevant person under paragraph 4 of this article may be postponed for not more than 12 months each time.

7. If, in the case determined by paragraph 6 of this article, a prosecutor delivers a final decision in a criminal case, a person, against whom the covert investigative actions have been carried out, shall be notified of the carrying out of the covert investigative actions immediately after the final decision.

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".

5.7.3.7 Supervision and oversight

It is very well established in the case-law of the ECtHR that due to the fact that surveillance of communications is exercised in secret, the risks of arbitrariness are evident.[132] It is therefore necessary that the state implements adequate safeguards against arbitrary application and abuse of the law. As explained by the ECtHR, "the overarching requirement is that a secret surveillance system must contain effective guarantees – especially review and oversight arrangements – which protect against the inherent risk of abuse and which keep the interference which such a system entails with the rights protected by Article 8 of the Convention to what is "necessary in a democratic society"".[133]

In this context, the ECtHR has explained that the relevant factors for deciding whether the oversight arrangements are adequate are (a) the independence of the supervisory authorities, their competences, and their powers (both to access materials and to redress breaches, in particular order the destruction of surveillance materials), and (b) the possibility of effective public scrutiny of those authorities' work.[134]

It also appears appropriate to differentiate here between oversight / supervision of specific cases, and systematic oversight of the operation of secret surveillance system as such. Regarding the first part, In Georgia oversight of surveillance measures is in the hands of several entities, including for start prosecutors, courts and the Personal Data Protection Service. There are several points to mention here:

- Courts control initiation of surveillance measures through authorization procedures. Next, they control execution of surveillance measures undertaken by the prosecutors in urgent circumstances. This includes also the cases where prosecutor concluded that intercepted material will not be used.
- As mentioned above, prosecutor is bound by law to terminate covert investigative action provided that conditions in the law are fulfilled (GeCPC Article 143^6).
- Next, covert investigative actions are also supervised by the Personal Data Protection Service. Also under conditions stipulated in the law, head of this service has the power to suspend such action (GeCPC Article 143^6).

Overall, the involvement of all of the abovementioned entities significantly reduces the risk of abusing the system in particular criminal cases.

But, there is also the other part of the oversight issue, and that is general control of the functioning of the system as a whole. Namely, the issue is whether system such as the one established in Georgia objectively reduces to a minimum the risk of any abuse, and not only that which can happen in the context of individual criminal proceedings.

[132] Zakharov v. Russia, paragraph 229.
[133] Ekimdzhiev and Others v. Bulgaria, paragraph 292.
[134] Ekimdzhiev and Others v. Bulgaria, paragraph 292 et seq.

The starting element here is that in Georgia, like in many other countries, relevant authorities have direct access to networks of communication service providers and are in the position to execute surveillance without further technical or legal participation of those providers (see more extensively 5.7.1 above). In such circumstances, it is important to consider also the oversight of system as a whole. Namely, while the control by prosecutors, courts and Personal Data Protection Service might be sufficient to prevent abuse in individual cases, there still remains a risk of misuse of system outside of specific criminal proceedings.

In this context, the following factors seem to be relevant:

In Georgia, body authorized to execute surveillance of communications is **LEPL – Operative-Technical Agency (OTA)**, which is an entity under subordination of the **Security Service of Georgia (SSSG)**. Head of the OTA is appointed directly by the Prime-Minister of Georgia, upon proposal of the Special Commission composed of representative of Government, Public Defendant, Head of Parliamentary Commission on Human Rights and Civil Integration, Head of Parliamentary Commission on Defence and Security, Head of Legal Commission of Parliament, Supreme Court Judge nominated by the Chairman of the Supreme Court, Head of SSSG – as a head of the Commission.

It is important to note here that in the past covert surveillance of the telephone conversations were possible in Georgia only by means of two-level, so-called "two-key" system, which preclude activation of objects without the consent of the other authorized entity, which before 2022 was the State Inspector. We were unable to verify whether this system, which contributes significantly to protection against abuse, is still in place. If it is, it should be seen as an important safeguard.

OTA and SSSG are subject to different level of control, but for the purposes of this report the most important is the one executed by the Parliament of Georgia, in accordance with the *Rules of Procedure of the Parliament of Georgia*.[135] Several forms of oversight are regulated in the Rules – (1) through the Committee of Defence and Security, (2) through **the Trust Group** and (3) through other field-specific committees.[136] The most relevant to the situation at hand is the one conducted by the Trust Group, since it is specifically tasked with overseeing authorities in the defence and security sector.

Trust Group is a subcommittee of the Defence and Security Committee. President of the Chair of the Defence and Security Committee of the Parliament is the chair of a Trust Group, and acts on behalf of the group.[137] Group is composed of five members in total, three of which are from the Majority, one from the Minority and one unaffiliated MP.[138] Decisions are made by majority of votes.[139]

In Georgia, MPs nominated for the membership in the Trust Group need to undergo security background check before they are confirmed by the Parliament. This check is conducted by the

[135] English translation available at http://old.parliament.ge/en/ajax/downloadFile/131641/ROP_as_of_27_Dec_2018_ENG.pdf.

[136] RPPG, Articles 156 *et seq.*

[137] RPPG, Article 157(7).

[138] RPPG, Article 157(2).

[139] RPPG, Article 158(1).

SSSG.[140] And according to the Law on State Secrets, decision to deny access to state secrets can be made on relatively vague grounds, i.e. if "the person prejudices or will prejudice the national and public security interests, the life and health of the population, and human rights and freedoms, based on the factual circumstances revealed as a result of the security background investigation and based on the low degree of trustworthiness and reliability". As noted by the Commissioner for Human Rights, there can be legitimated concerns about "parliamentarians being given access to highly sensitive information and particularly information about security service operations. Such concerns are more common in post-authoritarian countries and those that have secessionist political parties represented in parliament".[141] Therefore, some European states require prospective members of parliamentary oversight committees to be vetted and obtain a security clearance before taking their place on the committee.[142] But, this practice is seen as controversial, because it puts the security service in position "to vet their would-be overseers", which could be abused, but also because there is a broader issue of separation of powers between the executive branch and members of parliament, who have been selected by the electorate.[143]

Sittings of the group are held as necessary, upon the summon of the Chair. Individual member can suggest a meeting to be held, but he or she needs to gain support of at least two other members to summon a sitting. Hearings of the group are closed by default, but other MPs and persons from the defence and/or security sector may attend a sitting based on the decision of the Group (meaning majority of votes are necessary).

The most problematic issue here is that it appears that the scope of oversight by the Trust Group is severely limited. Pursuant to Article 159(1) of the RPPG, the "*Trust Group supervises secret activities and special programs in the Defense and Security sector, except for the activities relating to covert forms and methods of activity as prescribed by the legislation of Georgia*". In other words, the Trust Group is tasked with supervising all secret activities and special programs in the defence and security sector, **except the activities relating to covert forms and methods of activity**. The exception above is very broad in scope. Since "covert forms and methods of activity" could very well encompass different surveillance programmes, follows that these could be completely out of scope of oversight by the Trust Group. In such circumstances, it must be concluded that the secret surveillance programs in Georgia are not subject to effective oversight.

But, most importantly, it appears that OTA enjoys special exception from the obligation to provide information. To begin, we note that it is stipulated in the Article 159(2) of the Rules that "Respective authorities are obliged to provide all information to the relevant Trust Group necessary for the uninterrupted exercise of its powers, except for the cases envisaged by the legislation of Georgia. The Operative-Technical Agency provides information to a Trust Group as prescribed by paragraph 9 of this article". Second sentence of this paragraph creates a special position for the OTA, which is not (like other authorities) obliged to provide all information necessary for the work of the Trust Group. Instead, the OTA is obliged to provide information only as prescribed in paragraph 9. And pursuant to paragraph 9, "the Operative-Technical Agency, a legal entity of public law, shall submit a statistical and generalized report of performance annually". Other obligations of the OTA are not specified in paragraph 9. To sum

[140] Law of Georgia on State Secrets, articles 18 *et seq*.

[141] Commissioner for Human Rights 2015, p. 44.

[142] Commissioner for Human Rights 2015, p. 44.

[143] Commissioner for Human Rights 2015, p. 44.

up, under Georgian law activities OTA is under duty to provide to the Trust Group only annual report containing statistical and generalized report of performance.

Serious limitations are also imposed on the Trust Group vis-à-vis inspections of the OTA. Pursuant to the RPPG, members of the Trust Group are authorized, with the contest of the Chair, to visit the relevant authorities regarding issues within the competencies of the Trust Group, interview employees of the authority and get acquainted with information regarding issues within the competencies of the relevant Trust Group during the visit. But these visits cannot be unannounced, since the decision of the Chair must be sent to the relevant authority prior to the visit.[144] And when OTA is in question, the requirements are even stricter. Decision to visit and inspect the OTA needs to be made by the Trust Group (majority vote is required) instead of by the Chair, and more importantly, OTA cannot be inspected more than twice a year. Finally, the Trust Group selects only one of its members to conduct inspection.[145]

We consider this approach unsatisfactory. It appears that in practice the Trust Group only has power to read annual and generalized reports of the OTA, visit it very rarely (no more than twice a year) and only after the visit has been announced. We do not see rational reasons for such an approach, especially since members of the Trust Group need to have appropriate security clearance (see above section 2.4.2.2.). Moreover, limiting access to information to members of the oversight body who have appropriate security clearances was also flagged as problematic by the ECtHR.[146]

Moreover, pursuant to the case-law of the ECtHR, oversight bodies should also be competent to order remedial measures, and particularly to order that illegally obtained material be destroyed. In Georgia, the Trust Group has the right and the duty to, in cases where it identifies that a crime has been committed, inform the relevant investigative body. Moreover, it is authorized to present recommendations to the authorities of the defence and security sector of Georgia. Other than these, the Trust Group holds no other powers which would be capable of ensuring effective protection of fundamental rights and freedoms.

From the analysis above, we see that in addition to general limitations of the Trust Group's competences (see section 2.4.2.3. above), its powers are also severely restricted, in particular regarding accessing information and resources of the OTA. Consequently, we conclude that on the basis of this criteria as well, the oversight by the Trust Group is not effective.

5.8 Summary and recommendations

- GeLOIA makes it explicit that covert investigative actions defined therein can be executed only in line with the requirements in the GeCPC. Hence, we do not consider the fact that some powers are defined in multiple statutes as seriously problematic in itself.
- GeCPC prescribes reasonably foreseeably that electronic evidence can be used in criminal proceedings.

[144] RPPG Article 159(11).

[145] RPPG, Article 159(12).

[146] ECtHR, Ekimidzhiev and others vs. Bulgaria, paragraph 343.

- Georgian legislation properly distinguishes between categories of data defined in the Convention.
- Georgian legislation still does not implement preservation orders (Articles 16 and 17 of the Convention) as standalone measures. It is recommended that this be rectified, since these powers would additionally empower Georgian law enforcement authorities and at the same time would contribute to proper execution of procedural powers, in line with Article 15 of the Convention.
- Georgian legislation properly implements Article 18 of the Convention when it comes to production of computer data in general. Regarding production of subscriber information, Georgian legislation limits the application of domestic power investigations of criminal offences carried through a computer system, which is narrower than required by the Convention. While this is not in itself problematic from the perspective of Convention's Article 15, national authorities of Georgia might want to consider this and broaden the application of Article 136(2) so that power defined therein can be used when investigating any criminal offence.
- Search and seizure is regulated in a quality manner. Areas for possible improvement include prescribing different modalities for seizure of computer data in line with Article 19(3) of the Convention, as well as considering adding specific rules pertaining to matter regulated by Article 19(2) of the Convention (extended search).
- In the area of surveillance of communications, we note that Georgian legislation contains (GeLEC) clear obligations for the communication service providers regarding their assistance in the implementation of these powers. These duties are prescribed in a foreseeable manner and implement some safeguards. However, there are also some shortcomings, for instance with the logging obligation, which appears to be too narrow. Also, it is to be noted that Georgian authorities (OTA) have direct access to communication service providers, which creates additional risks of abuse. And while there are relatively good safeguards for the use of surveillance powers in individual cases under the GeCPC, it appears that Georgian system falls short of necessary European standards when systematic oversight is considered. This is mostly due to the fact that parliamentary control over the actions of the OTA is severely limited, and there are no alternative entities which can execute appropriate control. In the past there was the so-called double key infrastructure, which required additional authorization of surveillance orders by a separate state body. However, it is not clear at the time when this report was submitted how that system operates now. In any case, national authorities of Georgia might consider reforming their oversight systems and ensuring that they are in line with the relevant European standards.
- Powers of real-time collection of traffic data and interception of content data seem to be defined in precise and foreseeable terms. While there is some room for improvement regarding particular safeguards, overall, the GeCPC seems to implement the necessary safeguards.

6 Moldova

6.1 Relevant legal framework

This part of the report is based on the analysis of the following legislation:

1. Moldovan Code on Criminal Procedure (hereinafter: MdCPC)[147]
2. Moldovan Law on Preventing and Combating Cybercrime (hereinafter: MdLPCC)[148]
3. Moldovan Law on Special Investigative Activity (hereinafter: MdLSIA)[149]
4. Moldovan Electronic Communications Act (hereinafter: MdECA)[150]
5. Moldovan Law on the Intelligence and Security Service of the Republic of Moldova (hereinafter: MdLISS)[151]
6. Law on the Parliament Regulation (hereinafter: MdLPR)[152]

Since the last report (2018), there have been multiple changes in the legislation that governs the subject-matter analysed here. For the preparation of this document, we relied on their publicly available consolidated versions.

The purpose of this report is overall analysis of national legislation in the implementation of procedural powers of the Convention (Articles 16 to 21), from the perspective of conditions and safeguards used to ensure protection of fundamental human rights and freedoms (Convention's Article 15). And since the procedural powers in the Convention are used to collect evidence for the purpose of specific criminal investigations or proceedings (Article 14), the primary relevant sources of regulation in the domestic law are codes on criminal procedure. But, there are many secondary issues which can be regulated by other laws as well, and hence we attempted to pursue a broader approach and also look into those sources.

The following mapping indicates articles in the national legislation which were identified as either directly or indirectly relevant in the context of this report. It serves to get a better glimpse of the general legal landscape in the country.

In addition to the code on criminal procedure, Moldova also regulates some procedural powers in the Law on Special Investigative Activity (MdLSIA). This is characteristic for other countries analysed in this report as well. General observations made in relation to the concept of similar laws of other countries are equally relevant here. MdLSIA pursues relatively broad aims which go beyond investigations of specific criminal offences[153]. Multiple national authorities have the right to undertake measures prescribed in this law, including specialized subdivisions within the Ministry of Internal Affairs, the Ministry of Defense, the National Anti-Corruption Center, the

[147] Available at https://www.legis.md/cautare/getResults?doc_id=136769
[148] Available at https://www.legis.md/cautare/getResults?doc_id=133274
[149] Available at https://www.legis.md/cautare/getResults?doc_id=123543
[150] Available at https://www.legis.md/cautare/getResults?doc_id=136435
[151] Available at https://www.legis.md/cautare/getResults?doc_id=136435
[152] Available at https://www.legis.md/cautare/getResults?doc_id=136244
[153] MdLSIA, Article 2.

Intelligence and Security Service, the State Protection and Guard Service, the Customs Service, the State Fiscal and the National Penitentiary Administration.[154].

Procedural powers defined in the MdLSIA can broadly be categorized into (1) ordinary[155] and (2) special investigative powers[156]. Among the ordinary powers we do not identify any which would be relevant from the perspective of the Convention. On the other hand, there are several special investigative measures defined in the MdCPC which touch upon issues regulated by Articles 20 and 21 of the Convention (see below section 6.7).

6.2 General considerations

6.2.1 Status of electronic evidence

Moldovan law accepts computer data as electronic evidence. Firstly, the notion of evidence is defined in the Article 93 of the MdCPC, and it includes "documents", "audio or video recordings, photographs" as well as "the procedural documents in which the results of the special investigative measures and their annexes are recorded, including the transcript, photographs, recordings and others". Regarding the notion of "document", Article 157(1) of the MdCPC stipulates that "documents in any form (written, audio, video, electronic, etc.) originating from natural or legal official persons constitute material means of evidence, if circumstances that are important for the case are exposed or proven in them". Moreover, there are multiple provisions of the MdCPC which regulate the acquisition and use of specific types of computer data in criminal proceedings. These include:

- Interception and recording of communications[157]
- Monitoring of telegraphic and electronic communications connections[158]
- Collecting information from suppliers of electronic communications services[159]
- Identification of the subscriber, the owner or the user of a electronic communication system or of an access point to an information system[160]

Hence, it appears that reasonably foreseeable that electronic evidence is admissible under the MdCPC.

6.2.2 Categories of computer data recognized in the legislation

Looking at the totality of legislative acts which regulate matters falling within the subject-matter of procedural powers to combat cybercrime, we see that Moldovan law generally builds on the categories of computer data in line with the Convention. Most importantly, the notions of

[154] MdLSIA, Article 6(1).
[155] See more extensively in MdLSIA, Article 7.
[156] See more extensively in MDLSIA, Article 18 *et seq*.
[157] MdCPC Article 132^8 *et seq*.
[158] MdCPC Article 134^1.
[159] MdCPC Article 134^4.
[160] MdCPC Article 134^5.

"computer data", "traffic data", "subscriber information" and "service provider" have been defined in the MdLPCC in line with the Convention.

Notion of **IT data** is defined in line with the Convention, as "any representation of facts, information or concepts in a form suitable for processing in an IT system, including a program capable of determining the execution of a function by an IT system". In the same context, IT system is defined as "any isolated device or set of interconnected or connected devices that ensure or one or more elements of which ensure, by executing a program, the automatic processing of data", which is generally in line with the Convention's concept of computer system.[161]

Traffic data is according to the MdLPCC "any data related to a communication transmitted through an IT system, produced by this system as an element of the communication chain, indicating the origin, destination, itinerary, time, date, size, duration or type of underlying service".[162] This definition is in line with the Convention.

The concept of **user data** is defined in the MdLPCC as "any information, in the form of computer data or in any other form, held by a service provider, related to the subscribers of these services, other than the data related to traffic or content, and which allow establishing: the type of communication service used, the provisions technical measures taken in this regard and the service period; the subscriber's identity, postal or geographic address, phone number and any other contact number, as well as billing and payment data available under a contract or service arrangement; any other information regarding the location of the communication equipment, available under a contract or service arrangement, as well as any other data that can lead to the identification of the user".[163] This corresponds to the Convention's notion of "subscriber information".

Finally, the notion of service provider, which is defined in the MdLPCC as "any public or private entity that offers users of its services the opportunity to communicate through an IT system, as well as any other entity that processes or stores IT data for this communications service or for its users"[164] is also in line with the definition in the Convention.

6.3 Expedited preservation of stored computer data

Article 16 of the Convention (Expedited preservation of stored computer data) is implemented in the MdLPCC. Pursuant to Article 4(4)(b) of this law, the General Prosecutor's Office has the competence to order, at the request of the criminal investigation body or ex officio, "the immediate conservation of computer data or data related to computer traffic, against which there is a danger of destruction or alteration, under the conditions of legislation on criminal procedure".

It appears that this measure can be applied only "in the framework of criminal investigation", which serves as an additional safeguard. But it is not precisely clear what is the impact of the requirement that the measure is applied "under the conditions of legislation on criminal procedure", or to put it more precisely, which conditions from the MdCPC need to be fulfilled

[161] MdLPCC, Article 2.
[162] MdLPCC, Article 2.
[163] MdLPCC, Article 2.
[164] MdLPCC, Article 2.

here. Nevertheless, it appears that whichever condition might be applicable, it should only result in additional safeguards, and hence we do not see any problematic issues from the perspective of Convention's Article 15 here.

It appears however that the power of the MdLPCC General Prosecutor's Office to order preservation of stored computer data is not subject to time limitations prescribed by Article 16(2) of the Convention. While this is not a serious shortcoming, Moldovan authorities might nevertheless consider this and ensure that preservation obligation is appropriately limited in duration.

6.4 Expedited preservation and partial disclosure of traffic data

In cases where it is necessary to preserve traffic data in possession of a service provider, Moldovan authorities can rely on Article 7(1) of the MdLPCC, which stipulates that service providers are obliged:

> *…*
>
> *c) to execute, under conditions of confidentiality, the request of the competent authority regarding the immediate preservation of computer data or data related to computer traffic, against which there is a danger of destruction or alteration, for a period of up to 120 calendar days, in accordance with the national legislation.*
>
> *…*

We note that the abovementioned provision 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.

Moreover, Article 17(1)(b) of the Convention is implemented in Article 7(2) of the MdLPCC, which stipulates that

> *"if the data related to computer traffic is in the possession of several service providers, the requested service provider is obliged to immediately provide the competent authority with the information necessary to identify the other service providers".*

In these circumstances, we consider that Moldovan implementation of Article 17 of the Convention satisfies the standards elaborated in section 1 of this report. But there are several other provisions of the MdLPCC, which add some ambiguity here. Namely, pursuant to its Article 7(1)(f), service providers are also obliged to

> *to ensure the monitoring, supervision and preservation of traffic data, for a period of 180 calendar days, to identify service providers, service users and the channel through which the communication was transmitted;*

Although the wording is a bit ambiguous, it appears that Article 7(1)(f) of the MdLPCC introduces an obligation to proactively store (for a period of 180 days) some traffic data, which effectively means data retention obligation. 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:

> *to keep all the information available, generated or processed in the process of providing its own electronic communications services, necessary to identify and track the source of electronic communications, identify the destination, type, date, time and duration of the communication, identify the user's or the user's communications equipment another device used for communication, identifying the coordinates of the mobile communication terminal equipment and ensuring the presentation of this information to the authorized bodies under the law. The information related to mobile or landline services will be kept for a period of one year, and those related to the Internet network - for 6 months, at the end of which the mentioned information will be destroyed irreversibly, through automated procedures, with the exception of information and documents processed in accordance with art. 73 and of those which, according to the normative acts in force, are kept for a longer period. The retention obligation also refers to failed call attempts.*

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.

6.5 Production order

6.5.1 Production order for computer data in general

Moldovan legislation does not implement as a standalone procedural power the main part of Convention's Article 18, namely the one which calls for production of general computer data held by any natural and legal persons. In such circumstances, it appears necessary to use search and seizure measures, which is suboptimal 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.

6.5.2 Production order for subscriber information

In part where it relates to the production of subscriber information, Article 18 of the Convention is implemented in the MdLPCC. Article 7 of this law obliges service providers:

> *a) to keep records of service users.*

> *d) to present to the competent authorities, on the basis of a request made in accordance with the law, data related to users, including the type of communication and the service that the user benefited from, the method of payment for the service.*

The notion of "data about user" or "user data" is defined in Article 2 of the same statute in a manner compliant with the notion of subscriber information from the Convention (see above 6.2.2).

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). An 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.

6.6 Search and seizure of stored computer data

Search and seizure of stored computer data can be executed on the basis of provisions of Chapter III, Section 4 the MdCPC which regulate "search and seizure of objects and documents".[165] In this context, Article 125(1) of the MdCPC empowers criminal investigation bodies to undertake search for "documents that could be important for the criminal case and that cannot be obtained through other evidentiary procedures". Considering that the notion of "document" includes computer data, and also considering that paragraph 2 of this article additionally specifies that the search may also be carried out for the purpose of discovering "data important for the criminal case", we do not see any issues with these provisions from the perspective of legal foreseeability.

Moldovan legislation contains an important safeguard in Article 125(1), which prescribes that search can be undertaken when documents important for the criminal case cannot be obtained through other evidentiary procedures.

In procedural terms, search must be based on a reasoned order of the criminal investigative body and the authorization of the investigative judge.[166] The same is also true for seizure.[167] Only in the case of "flagrant crime", a search may be based on a reasoned order without the 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.[168] 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.[169]

There are no specific rules in the MdCPC addressing extended search in line with the Article 19(2) of the Convention. But, it seems important to note that MdCPC stipulates that "it is forbidden to carry out searches exceeding the premises, in other places, on the basis of other acts or pursuing other purposes than those indicated in the conclusion of the investigating judge regarding the authorization or in the prosecutor's order".[170] If this provision would be applicable to computer data, it appears that extended search would be possible only with additional authorization of the court.

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. In this context, it appears that since the last assessment the MdCPC was amended by several new provisions in Article 128. These read as follows:

> *5[1]) The collection of objects, documents, data storage devices or information systems in the original is allowed only if, after the on-site examination, in advance, it is established that they could have express and indispensable*

[165] MdCPC, Article 125 *et seq*.
[166] MdCPC, Article 125(3)
[167] MdCPC, Article 126(3)
[168] MdCPC, Article 125(4)
[169] MdCPC, Article 125(4, 5)
[170] MdCPC, Article 128(2).

importance for the criminal case, and their lifting does not inevitably stop the economic activity of the person.

(5[2]) If the collection of objects, documents, data storage devices or information systems in the original is not possible without the inevitable stoppage of the economic activity of the person, the criminal investigation body orders, by reasoned ordinance, the making of copies and photo recordings or video, data storage, inspection, measurement or sampling, which serve as evidence. Making copies and photo or video recordings, storing data (cloning of information systems), inspecting, measuring or taking samples is carried out, as the case may be, with the participation of the specialist, by using methods and technical means that ensure the integrity and authenticity of documents, objects, devices data storage or information systems.

(5[3]) If it is impossible to make copies and photo or video recordings, data storage (cloning of information systems), inspection, measurement or sampling of objects, documents, data storage devices and information systems at the place of carrying out the procedural action without affecting their integrity and authenticity or their possessor does not allow or obstructs the carrying out of these actions, the criminal investigation body raises them for the purpose of making copies and photo or video recordings, data storage (cloning of information systems), inspection, measurement or sampling, indicating in the report the individualization elements of each object, document or device.

(5[4]) In all cases, with the exception of ordering technical-scientific findings or judicial expertise on objects, documents, data storage devices or information systems, they shall be returned to the person from whom they were taken within 3 days of upon lifting. If due to the individual properties of the objects, documents, data storage devices or information systems, more time is required for their examination, the return term can be extended by the reasoned order of the prosecutor, but not more than for a total term up to 20 days from the date of collection.

In our opinion the abovementioned provisions are a welcome addition in the MdCPC. Although the language used here is somewhat different from that in the Article 19(3) of the Convention, these rules make it explicit that law enforcement authorities must execute search and seizure in the way which is most proportionate and sensitive of the data holder's interests. This contributes significantly to application of Article 15(3) of the Convention, which stipulates that "to the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties".

In 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)[171];

- 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).

Overall, we do not identify serious shortcomings in the Moldovan legislation regarding application of Convention's Article 15 to search and seizure.

6.7 Surveillance of communications

6.7.1 Duties of service providers to assist in the surveillance of communications

In Moldova, providers of electronic communications networks and/or services are generally obliged under the MdECA "to allow, from a technical point of view, the authorized bodies to carry out, under the law, operative investigative measures on electronic communications networks and to present the necessary technical data for this purpose".[172] But, MdECA does not regulate this obligation beyond imposing this general duty.

While it is generally clear from this provision that Moldovan service providers are under the duty to "allow" authorized bodies to execute surveillance measures, it is not clear which national bodies are empowered to request such assistance, nor what is the precise scope of service providers' obligations. In particular, MdECA does not stipulate whether such assistance goes to the level of putting authorized bodies in the position of conducting surveillance autonomously without further technical assistance from the service providers. But, it is stipulated in Article 7(e) the MdLISS that the Security Service of Moldova performs "the technical assurance of interception of communications made using electronic communications networks using special software or technical means installed or connected, where necessary, to the equipment of providers of electronic communications networks and/or services". Hence, since it appears reasonably clear that the Security Service might have direct access to communications, it is

[171] MdCPC Article 127.
[172] MdECA Article 20(3)(b)

obvious that Moldovan law should also include relevant safeguards. For comparison, approach used by the Georgian legislators (see section 5.7.1 above) might be analysed.

It is also to be noted that, at the time when this report was prepared, Moldovan authorities were preparing the draft of the new Law on the Intelligence and Security Service, which explicitly regulates some of these matters. This draft was analysed in detail by the experts of the Venice Commission, who raised multiple concerns regarding the possible interferences of fundamental human rights.[173]

In any case, Moldovan legislation currently in force does not define with sufficient clarity the scope of obligations for the communication service providers when it comes to their role in the implementation of surveillance measures.

6.7.2 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);*

[173] See the Draft law at https://www.venice.coe.int/webforms/documents/?pdf=CDL-REF(2023)001-e and the Opinion of the Venice Comission CDL-AD(2023)008.

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[174] and authorized[175] 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 (6.7.3).

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.

6.7.3 Interception of content data

6.7.3.1 Legal basis for interception of content data in domestic legislation

Legal basis for interception of communication content data is found in Section 5 (Article 132 *et seq*) of the MdCPC and Article 18 of the MdLSIA. Under both statutes, interception of communications is defined as one of the special investigative activities.

In the context of the MdCPC, actions broadly touching upon interception of content are listed in Article 132^2(1)(1) and include:

- interception and recording of communications or images,[176]
- detaining, investigating, surrendering, searching or picking up postal items,[177]
- monitoring telegraphic and electronic communications connections[178] and

[174] MdLSIA, Article 18(3).
[175] MdLSIA, Article 20(1).
[176] MdCPC, Article Article 132(1)(1)(c)
[177] MdCPC, Article Article 132(1)(1)(d)
[178] MdCPC, Article Article 132(1)(1)(e)

- collecting information from providers of electronic communications services[179].

Pursuant to Article 132[8](1) of the MdCPC, "the **interception and recording of communications** presupposes the use of technical means through which the content of conversations between two or more people can be found, and their recording presupposes the storage of the information obtained as a result of the interception on a technical medium". 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 "**detention, investigation, surrender, search or seizure of postal items**", the wording and overall scheme of MdCPC 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 telegraphic and electronic communications connections**", includes, pursuant to Article 134[1], "access and verification without notifying the sender or the recipient of the communications that were sent to the institutions that provide services for the delivery of electronic correspondence or other communications and the incoming and outgoing calls of the subscriber".

Finally, "**collecting information from suppliers of electronic communications services**" implies both the interception of content data and real-time collection of traffic data. As regards interception of content data, this power covers "collection from telecommunications institutions, from fixed or mobile telephone operators, from Internet operators of information transmitted through technical telecommunications channels (telegraph, fax, paging, computer, radio and other channels), the secret recording of information transmitted or received through the technical lines of telecommunications links by the persons subject to the special investigation measure".

Considering all of the above, we note that subject-matters and delineation of above-mentioned measures are not sufficiently clear. For instance, it is not easy to understand what is the relation between Articles 133 and 134[1] in those cases 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 one provision which would create legal basis for interception of all computer data which are transmitted as content of some communication would provide necessary precision.

Moreover, in addition to the abovementioned provisions of the MdCPC, 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,

[179] MdCPC, Article Article 132(1)(1)(h)

(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.

We note with satisfaction that Moldovan legislation stipulates precisely that above-mentioned special investigative actions are performed[180] and authorized[181] 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).

6.7.3.2 Authorization procedure

Regarding authorization procedure, it is important to note that 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.[182] 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.[183] 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.

Next, we look at the authorization authority's scope of review. As explained in the introduction, the ECtHR has held that this authority 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

[180] MdLSIA, Article 18(3).
[181] MdLSIA, Article 20(1).
[182] MdCPC, Article 132^4(3).
[183] MdCPC, Article 132^4(3).

this is to ensure that "*secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration*".[184]

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 in 2018, 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.

6.7.3.3 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.*

[184] Zakharov v Russia, ECtHR app. no. 47143/06, para 257.

> *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) The communications of the suspect, the accused or other persons, including those whose identity has not been established, about whom there is data that can reasonably lead to the conclusion that they either contribute, in any way, to the preparation, may be subject to interception and recording , committing, favoring or concealing the crimes provided for in para. (2), either receive or transmit relevant and important information for the criminal case.*
>
> *(4) The communications of the victim, the injured party, his relatives and family members, as well as the witness, may be subjected to interception and recording, if there is imminent danger to his life, health or other fundamental rights, if it is necessary to prevent the crime or if there is an obvious risk of irretrievable loss or distortion of the evidence. The interception and recording of communications for the purposes of this paragraph is ordered according to the procedure provided for in art. 132 [4] and only with the written consent or prior written request of the persons indicated in this paragraph. The measure ordered according to this paragraph is to be terminated immediately after the disappearance of the basis that was the basis of its authorization or at the express request of the person in respect of whom 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".

6.7.3.4 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".[185]

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*".*[186]

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".*[187]

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".*[188]

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.[189] 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.

6.7.3.5 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

[185] Zakharov v Russia, para 250.
[186] MdCPC, Article 132^4(7).
[187] MdCPP, Article 132^4(6).
[188] MdCPP, Article 132^4(8).
[189] MdCPP, Article 132^4(9).

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".[190]

- "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".[191]
- "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".[192]
- 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. [193]
- 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 communications. A verbatim record of the communications important for the criminal case shall be attached to the transcript.[194]
- 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.[195]
- 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

[190] MdCPC, Article 132^9(1).
[191] MdCPC, Article 132^9(4).
[192] MdCPC, Article 132^9(5).
[193] MdCPC, Article 132^9(6).
[194] MdCPC, Article 132^9(8).
[195] MdCPC, Article 132^9(13).

investigative judge shall be recorded by the responsible person in the transcript attached to the criminal case file.[196]

6.7.3.6 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.*

6.7.3.7 Oversight

It is very well established in the case-law of the ECtHR that due to the fact that surveillance of communications is exercised in secret, the risks of arbitrariness are evident.[197] It is therefore necessary that the state implements adequate safeguards against arbitrary application and abuse of the law. As explained by the ECtHR, "the overarching requirement is that a secret surveillance system must contain effective guarantees – especially review and oversight arrangements – which protect against the inherent risk of abuse and which keep the interference which such a system entails with the rights protected by Article 8 of the Convention to what is "necessary in a democratic society"".[198]

It appears appropriate to differentiate here between supervision in specific cases, described in the sections above, and systematic oversight of the operation of secret surveillance system as such.

In this context, the ECtHR has explained that the relevant factors for deciding whether the oversight arrangements are adequate are (a) the independence of the supervisory authorities, their competences, and their powers (both to access materials and to redress breaches, in particular order the destruction of surveillance materials), and (b) the possibility of effective public scrutiny of those authorities' work.[199]

---

[196] MdCPC, Article 132^9(15).
[197] Zakharov v. Russia, paragraph 229.
[198] Ekimdzhiev and Others v. Bulgaria, paragraph 292.
[199] Ekimdzhiev and Others v. Bulgaria, paragraph 292 et seq.

The starting element here is that it appears that in Moldova, like in many other countries, relevant authorities have direct access to networks of communication service providers and are in the position to execute surveillance without further technical or legal participation of those providers (see more extensively 6.7.1 above). In such circumstances, it is important to consider also the oversight of system as a whole.

Unfortunately, we have been able to identify only a limited number of provisions in the Moldovan legislation relevant for this issue.

When it comes to the oversight of the Security Service of Moldova MdLISS stipulates:

- that control over the Service's activity is exercised by the Parliament, the Prosecutor's Office and the courts, within the limits of their competence[200]
- that the service presents, in the manner established annually, by June 1, and in case of necessity upon request, to the Parliament in plenary session, to the President of the Republic of Moldova and to the Government, reports on the performance of its activity[201]
- that parliamentary control over the Service's activity is carried out by the National Security Commission, according to its regulations[202]

This is further elaborated in the MdLPR, which contains specific rules on the work of the Subcommittee for the exercise of the parliamentary control the Service's activity of Information and Security (Article 28). Pursuant to this article,

> *(1) Within the Commission for national security, defence and public order, a subcommittee is active for the exercise of parliamentary control over the activity of the Intelligence and Security Service (SIS).*
>
> *(2) A representative of the parliamentary opposition is elected as the president of the subcommittee.*
>
> *(3) The subcommittee supervises the observance by SIS of the legality, fundamental rights and freedoms of man and the democratic order in the state, ensures that the political engagement of SIS is not admitted.*
>
> *(4) The subcommittee verifies compliance by the SIS with the provisions of the Constitution and the laws that regulate the activity of the SIS, examines cases of violation of the Constitution, the laws, the constitutional rights and freedoms of citizens.*
>
> *(5) The members of the subcommittee have access to secret information, signing, in each separate case, a commitment to preserve the confidentiality of information that constitutes a state secret, bearing responsibility in accordance with the legislation.*
>
> *(6) The members of the subcommittee may request, with the agreement of its president, secret information and information regarding the current activity of the SIS, with the exception of information regarding the operative activity of*

[200] MdLISS Article 20(1).
[201] MdLISS Article 20(2).
[202] MdLISS Article 20(2).

> *the service or the identity of persons who work undercover, being part of the script staff or having specific missions that require non-disclosure of identity.*

In Moldova, parliamentary oversight of the Security Service according to the current legislation appears to be unsatisfactory. While the solution of the Moldovan parliament according to which MP from the opposition is elected as the president of the relevant committee is certainly welcome since it helps to build trust, the fact remains that the subcommittee is not provided with adequate powers. According to the standards of the ECtHR, parliamentary committees exercising control overs agencies in charge of surveillance should be independent, have adequate powers, be subject to public scrutiny. And while members of the Moldovan parliamentary control body have the power to get necessary information, they are not provided with additional powers such as the one to conduct on site inspections and visits, to use external experts, to get unfettered access to all necessary information, to order illegalities to be remedied, etc.

Also, in this context we note that the Venice Commissions assessed that parliamentary control in Moldova

> *… appears rather superficial as the Sub-Committee seems to have a simply statistical role, 34 being excluded from a proper supervision of relevant activities of the SIS, including special files and pending operations. Although members of the parliamentary subcommittee may submit questions about the intelligence/counterintelligence activity carried out by the Service in the previous year, this may be made ineffective since information on ongoing operations explicitly excluded from the report and, according to the information provided by the Sub-Committee during the online meetings, the SIS has the right to refuse access to any information by asserting the State secret. The role of the SubCommittee is consequently reduced to the production of a yearly report, which is not necessarily published.*[203]

6.8 Summary and recommendations

- Some procedural powers in the Moldovan law are regulated by the MdLSIA, which (as is the case in other surveyed countries) pursues much broader aims than those of the MdCPC and the Convention. These include production orders for subscriber information and real-time collection of traffic data. However, it appears that actions of law enforcement authorities on the basis of these two statutes are adequately delineated. Hence, we do not find any serious issues which would be relevant from the perspective of Article 15 in this context.
- MdCPC reasonably foreseeably prescribes that electronic evidence can be used in criminal proceedings.
- Moldovan legislation properly differentiates between various categories of data which are recognized by the Convention. This creates a basis for adequate differentiation of procedural powers in the MdLPCC and the MdCPC. Definitions of IT data (corresponding to computer data), traffic data, user information (corresponding to subscriber information) and service provider are generally compatible with the ones in the Convention.

[203] Opinion of the Venice Comission CDL-AD(2023)008, p. 10.

- Moldovan legislation implements Article 16 of the Convention in an adequate manner. Although there are some minor shortcomings, these do not seriously bring compliance with Article 15 into question.
- Moldovan legislation properly implements Article 17 of the Convention. Some minor differences regarding preservation periods do not seriously compromise compliance with Article 15.
- There seem to exist some discrepancies in the legislation regulating data retention. National authorities might reassess whether provisions of different laws which create obligations for communication service providers are consistent with each other. Also, it would be best to avoid regulating the same matter in different legislative acts.
- Article 18 is implemented generally in line with the Convention when it comes to production of subscriber information. On the other hand, production of computer data in general is not regulated as a standalone procedural power.
- Article 19 of the Convention is in general implemented in an appropriate manner. National authorities might consider adding specific rules in the national legislation which would regulate matters covered by Article 19(2). Recent amendments of the MdCPC make it more compliant from the perspective of Article 19(3) of the Convention.
- It appears that Moldova uses the legal and technical system in which communication service providers are obliged to assist the Security Service to intercept communications, which includes their obligation to install special hardware and software for these purposes. Such a system, while not problematic in itself, might be particularly prone to abuse and hence needs to be subject to effective oversight. Unfortunately, it appears that the oversight mechanisms currently prescribed in the MdLSIA and the MdLPPD are not adequate.
- There seems to exist an appropriate legal basis for real-time collection of traffic data. Some minor clarifications in the law might still be necessary.
- Rules on interception of content data in general implement necessary safeguards. Some minor clarifications in the law might still be necessary.
- Moldova does not appear to implement effective oversight of secret surveillance system. This might be viewed as one of the priorities for future legislative amendments.

7 Ukraine

7.1 Relevant legal framework

This part of the report is based on the analysis of the following legislation:

1. Ukrainian Code on Criminal Procedure (hereinafter: UaCPC)[204]
2. Ukrainian Law on Electronic Communications (hereinafter: UaLEC)[205]
3. Ukrainian Law on Operational and Investigative Activities (hereinafter: UaLOIA)[206]
4. Ukrainian Law on the Security Service of Ukraine (hereinafter: UaLSS)[207]
5. Regulations of the Verkhovna Rada of Ukraine (UaRVR)[208]

Since the last report, there have been multiply changes in the legislation that governs the subject-matter analysed here. Ukrainian Code on Criminal Procedure from 2012 undertook several additional changes, with the most recent ones in 2022 and 2023. Majority of these changes have been made to address specific issues and circumstances resulting from the aggression by the Russian Federation, while some are of a more general nature.

The purpose of this report is overall analysis of national legislation in the implementation of procedural powers of the Convention (Articles 16 to 21), from the perspective of conditions and safeguards used to ensure protection of fundamental human rights and freedoms (Convention's Article 15). And since the procedural powers in the Convention are used to collect evidence for the purpose of specific criminal investigations or proceedings (Article 14), the primary relevant sources of regulation in the domestic law are codes on criminal procedure. But, there are many secondary issues which can be regulated by other laws as well, and hence we attempted to pursue a broader approach and also look into those sources.

7.2 General considerations

7.2.1 Applicable national legislation

As is the case with other jurisdictions analysed in this report, Ukrainian law also regulates procedural powers of the law enforcement agencies in several laws, with the basic differentiation between rules of the UaCPC and the rules in the UaLOIA. As elsewhere, UaLOIA pursues broader list of aims, which include finding information about the illegal actions of individuals and groups, the responsibility for which is provided for by the Criminal Code of Ukraine, intelligence and subversive activities of special services of foreign countries and organizations with the aim of stopping offenses and in the interests of criminal justice, as well as obtaining information in the interests of the safety of citizens, society and the state[209]. It also appears that provisions of the UaLOIA are applicable in the context of international cooperation in the field of investigative

[204] Available at https://zakon.rada.gov.ua/laws/show/en/4651-17/ed20231106#Text
[205] Available at https://zakon.rada.gov.ua/laws/show/en/1089-20#n2142
[206] Available at https://zakon.rada.gov.ua/laws/show/en/2135-12#Text
[207] Available at https://zakon.rada.gov.ua/laws/show/en/2229-12/conv#n272
[208] Available at https://zakon.rada.gov.ua/laws/show/en/1861-17#n22
[209] UaLOIA Article 1.

activities[210]. It is important to emphasize that the UaLOIA defines many procedural powers[211] whose execution is generally independent of the rules in the UaCPC. But it is likewise important to underline that procedural powers which are subject to the analysis in this report do not fall into this category, as they can be executed only in accordance with the rules of the UaCPC.[212]

7.2.2 Status of electronic evidence

Pursuant to Article 84(2) of the UaCPC, procedural sources of evidence are testimonies, physical evidence, documents and expert findings. Moreover, according to Article 99(2)(1) of the UaCPC, documents may be "materials of photography, sound recording, video recording and other data media (including electronic ones)". Hence, we consider it reasonably foreseeable that electronic evidence is generally admissible under the UaCPC.

7.2.3 Categories of computer data recognized in the legislation

As is mentioned repeatedly in this report, Convention differentiates not only between various procedural powers, but also in terms of categories of computer data which can be subject to those powers. Differentiation of categories of data is therefore an important element for the proper implementation of procedural powers, and in turn also for proper implementation of the principle of proportionality.

Ukrainian legislation does not define the notion of **traffic data**. To be sure, UaLEC indirectly relies on this concept in its Article 121 where it provides for rules on "access to information about the consumer, the facts of the provision of electronic communication services, including data processed for the purpose of transmitting such information in electronic communication networks". But it is not precisely clear from the legislation which specific categories of data fall within this category. Likewise, as will be explained below, Article 263(3) of the UaCPC speaks about "collecting information from transport telecommunication networks" includes the "receiving, converting and recording various types of signals transmitted by communication channels". But it is once again left undefined which information or "carious types of signals" those might be. We consider that national authorities of Ukraine might consider these issues and ensure that scope of procedural powers regarding traffic data is regulated more precisely, by making it explicit which categories of data are subject to relevant procedural powers.

Likewise, the notion of **subscriber information** is also left undefined. UaCPC consequently treats subscriber information as any other computer data.

7.3 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. In such circumstances, national law enforcement authorities rely on procedural powers broadly corresponding to the production order in order to ensure preservation of stored computer data (see more extensively section 7.5 below). This is in line with the earlier assessment (in 2018), as well with explanations provided by national

[210] UaLOIA Article 5^1.
[211] UaLOIA Article 8.
[212] UaLOIA Article 8.

stakeholders at that time. National authorities might want to consider implementing Article 16 of the Convention as a specific and standalone power, for the following reasons:

- It would enable law enforcement authorities to choose between different procedural powers and to use the one which is the most appropriate in the circumstances, which is one of the aims of the Convention.
- Above approach would contribute to the principle of proportionality, which is explicitly provided in the Article 15 of the Convention.
- It would enable national law enforcement authorities to better participate in international data exchanges in line with the Convention.
- It would enable business entities to cooperate with law enforcement authorities on the basis of clear legal framework, which would be more in line with personal data protection principles.

7.4 Expedited preservation and partial disclosure of traffic data

Ukrainian law also does not recognize expedited preservation and partial disclosure of traffic data as a standalone procedural power. Hence, legal possibilities of securing data using the rules on provisional access (see 7.3 above and 7.5 below) also apply to traffic data.

Additionally, we were unable to identify specific rules on communication data retention in the UaLEC. It appears that the UaLEC provides only the obligation for providers of electronic communication services to keep reliable records of electronic communication services provided by them.[213] However, it seems that this obligation is meant to be used for civil law purposes (billing), since it is prescribed that records are kept "during the statute of limitations period defined by law". In any case, it is not specified precisely which records are to be retained on the basis of this provision. Hence, the situation here remains substantially unchanged compared to last assessment. At that time, representatives of private sector considered data retention rules to be imprecise, unforeseeable, and disproportional. In particular, it was argued that it is not sufficiently foreseeable what is the scope of the phrase "records" in Article 39(7) of the Law on Telecommunications, which was in force at that time. A similar argument can be made also in the context of equivalent obligation under Article 105 of the UaLEC.

Rules on access to data held by providers of electronic communications services are analysed below (see sections 7.5, 7.7 and 7.8).

7.5 Production order

7.5.1 Production order for computer data in general

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,

[213] UaLEC Article 105(8)(1).

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. Temporary access to things and documents consists in providing a party to criminal proceedings by a person in possession of such things and documents, the opportunity to get acquainted with them, make copies of them and remove them (seize them).*
>
> *Temporary access to electronic information systems, computer systems or their parts, mobile terminals of communication systems is carried out by removing a copy of the information contained in such electronic information systems, computer systems or their parts, mobile terminals of communication systems, without removing them.*

Second paragraph of this Article was amended in 2022 by adding specific references to computer systems.

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 specified in the decision of the investigating judge, court on temporary access to things and documents as the owner of things or documents, is obliged to provide temporary access to the things and documents specified in the decision to the person specified in the corresponding decision of the investigating judge, court.*

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

> *3. A person presenting a decision on temporary access to things and originals or copies of documents is obliged to leave to the owner of things and originals or copies of documents a description of things and originals or copies of documents that were seized in order to fulfill the decision of the investigating judge or court.*

and paragraph 4 of the same article provides that

> *4. At the request of the owner, the person presenting the decision on temporary access to things and documents must leave a copy of the seized original documents. Copies of documents that are removed or the originals of which are removed are made using copying equipment, electronic means of the owner (with his consent) or copying equipment, electronic means of the person who presents the decision on temporary access to things and documents.*

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.[214] Also, as noted above, UaCPC does not differentiate between various categories of computer data.

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.[215] 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 things and documents are or may be in the possession of the relevant natural or legal entity;*
>
> *5) the importance of things and documents for establishing circumstances in criminal proceedings;*
>
> *6) the possibility of using information contained in things and documents as evidence, and the impossibility of proving by other means the circumstances that are supposed to be proved with the help of these things and documents, in the case of submitting a petition for temporary access to things and documents that contain a secret protected by law;*
>
> *7) substantiation of the need to seize things and originals or copies of documents, if the relevant 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. The investigating judge, the court issues a decision on granting temporary access to things and documents, if the party to the criminal proceedings proves in its motion that there are sufficient grounds to believe that these things or documents:

> *1) are or may be in the possession of the relevant natural or legal entity;*
>
> *2) by themselves or in combination with other things and documents of the criminal proceedings, in connection with which the petition is submitted, are essential for establishing important circumstances in the criminal proceedings;*
>
> *3) do not constitute or include things and documents that contain secrets protected by law.*

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

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.*

7.5.2 Production order for subscriber information

There are no specific rules for production of subscriber information in the UaCPC. Addressing these shortcomings and making appropriate amendments would also contribute to quality of legislation and consequently compliance with Article 15.

7.6 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. No one has the right to enter a person's home or other possessions for any purpose, other than only with the voluntary consent of the person who owns them, or on the basis of the decision of the investigating judge, except for the cases established by part three of this article.*
>
> *2. A person's home means any premises that is in the permanent or temporary possession of a person, regardless of its purpose and legal status, and is adapted for the permanent or temporary residence of natural persons in it, as well as all the components of such premises. Premises specially designed for the maintenance of persons whose rights are limited by law are not housing. Other property of a person means a vehicle, a plot of land, a garage, other buildings or premises for household, service, economic, industrial and other purposes, etc., which are in the possession of a person.*
>
> *3. The investigator, inquirer, prosecutor has the right to enter the home or other property of a person before the decision of the investigating judge is issued only in urgent cases related to saving lives and property or direct prosecution of persons suspected of committing a criminal offense. In such a case, the*

> *prosecutor, investigator, inquirer, in agreement with the prosecutor, is obliged to apply to the investigating judge immediately after taking such actions with a request to conduct a search. The investigating judge considers such a petition in accordance with the requirements of Article 234of this Code, checking, among other things, whether there were really grounds for breaking into a person's home or other property without a decision of the investigating judge. If the prosecutor refuses to agree to the request of the investigator, the inquirer for a search or the investigating judge refuses to grant the request for a search, the evidence established as a result of such a search is inadmissible, and the obtained information is subject to destruction in the manner provided for in Article 255 of this Code .*

In such circumstances, search is executed on the basis of investigating judge's ruling,[216] which is made upon request of the public prosecutor or investigator (pre-approved by public prosecutor). Pursuant to Article 234(5),

> *5. The investigating judge refuses to grant a request for a search if the prosecutor or the investigator does not prove that there are sufficient grounds to believe that:*
>
> *1) a criminal offense was committed;*
>
> *2) the wanted items and documents are important for the pre-trial investigation;*
>
> *3) the information contained in the searched items and documents may be evidence during the trial;*
>
> *4) the wanted things, documents or persons are located in the residence or other property of the person specified in the petition;*
>
> *5) under the established circumstances, a search is the most expedient and effective way of finding and seizing things and documents that are important for a pre-trial investigation, as well as establishing the location of wanted persons, as well as a measure proportionate to the interference in a person's personal and family life.*

Sub-paragraph 5 quoted above is a new safeguard in the UaCPC (compared to the situation during last assessment).

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,

> *It is not allowed to conduct investigative (search) actions at night (from 10 p.m. to 6 a.m.), except in urgent cases when a delay in conducting them may lead to the loss of traces of a criminal offense or the escape of a suspect, as well as in addition to conducting criminal proceedings in according to the procedure established by Article 615 of this Code.*

In this context, we also note that according to Article 236(2),

[216] UaCPC, Article 234(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. Temporarily seized may be property in the form of things, documents, money, etc., regarding which there are sufficient grounds to believe that they:*
>
> *1) sought out, manufactured, adapted or used as means or instruments of committing a criminal offense and (or) retained its traces;*
>
> *…*

Foreseeability of the notion "documents" was already addressed above. 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.*

Finally, we did not identify rules covering matter addressed by Article 19(2) of the Convention.

7.7 Surveillance of communications

7.7.1 Duties of service providers to assist in the surveillance of communications

According to Ukrainian legislation, providers of electronic communication services bear responsibility for or the safety of data regarding their end users, obtained both on the basis of service contract and in the provision of services. Providers are generally under the obligation to protect privacy of their users, which covers both content and traffic data (including location data) associated with their communications (UaLEC, Article 119).[217] This information may be disclosed only with the user's consent or under conditions stipulated in the law (UaLEC Articles 119 and 121).

When it comes to the execution of surveillance measures, Ukrainian legislation creates an obligation for communication service providers to support activities of the law enforcement. Hence, UaLEC prescribes in Article 121, dealing with "conditions for providing access to information in cases provided for by law", that

> *2. The removal of information from electronic communication networks of providers of electronic communication services is ensured by a single system of technical means used by all legally authorized bodies, under the conditions of autonomous access to information in the manner determined by legislation.*
>
> *3. The provider of electronic communication services and/or networks must ensure the possibility of connecting the technical means specified in part two of this article at the point for such access in the electronic communication network specified by the provider of electronic communication networks and/or services.*

Hence, it is obvious from the abovementioned provisions that Ukrainian legislation, similarly to other jurisdictions analysed in this report, creates conditions for autonomous execution of

217

surveillance powers by the authorized state bodies. But it is not precisely clear from the UaLEC which state bodies are legally and technically provided with this autonomous access. In this context it appears from the provisions of the UaLSS that the Security Service of Ukraine has the right and the duty to "perform the function of technical regulation in the field of special technical means for removing information from communication channels and other technical means of secretly obtaining information" (UaLSS Article 24(19)).

7.7.2 Types of surveillance activities recognized in the legislation

Surveillance of communications is regulated by Section 2 of Chapter 21 of the UaCPC, dealing with covert investigative actions which interfere with private communications. Pursuant to Article 258(4) of the UaCPC, the following are actions which interfere in private communications:

> *1) audio, video monitoring of an individual.*
>
> *2) arrest, examination and seizure of correspondence.*
>
> *3) collecting information from telecommunication networks.*
>
> *4) collecting information from electronic information systems.*

First two of these measures appear to be unrelated to matters covered by Article 21 of the Convention. Namely, audio, video monitoring of an individual appears to cover conversations, sounds and movements of a person which are not transmitted by communications means, and arrest of correspondence covers pursuant to specific provision of the AmCPC (Article 261(4)) communication by postal packets, parcels, postal containers, postal money orders, telegrams, and other material mediums for exchange of information among individuals. Hence, in the remaining part of this report we focus on third and fourth of the abovementioned powers.

In this context, it is important to note that it appears that UaLOIA does not contain separate grounds for surveillance of communications. Instead, in the UaLOIA reference is made to relevant provisions of the UaCPC, which serves to avoid ambiguities as to which statute might be applicable in particular circumstances.[218]

7.7.3 Real-time collection of traffic data

It appears that Article 121 of the UaLEC recognizes the possibility of collecting various information generated in the context of communications, other than its content. Namely, pursuant to paragraph 1 of this article, "access to information about the consumer, the facts of the provision of electronic communication services, including data processed for the purpose of transmitting such information in electronic communication networks, is carried out exclusively on the basis of the decision of the prosecutor, the court, the investigating judge in the cases and procedure provided for by law".

It is to some extent vague what is the exact procedural power for real-time collection of traffic data, and also what is its scope. On the one hand, Article 258(4) of the UaCPC stipulates that "interference in private communication implies access to the contents of communication". It would follow that procedural powers mentioned above (section 7.7.2) cover only those cases where content of communications is being accessed by law enforcement authorities. On the

[218] See for instance Article 8 of the UaLOIA.

other hand, Article 263(3) of the UaCPC, which should be seen as more specific provision, stipulates that "collecting information from transport telecommunication networks" includes the "receiving, converting and recording various types of signals transmitted by communication channels". In any case, it appears that real-time collection of traffic data could also be covered by Article 264 of the UaCPC, which deals with "collection of information from electronic information systems". Nevertheless, we consider that Ukrainian legislation could be substantially improved if the power of real-time collection of traffic data would be introduced using more specific language. In particular, national authorities might consider defining precisely which categories of information are subject to real-time collection of traffic data.

7.7.4 Interception of content data

7.7.4.1 Legal basis

Article 21 of the Convention is implemented in Article 263 of the UaCPC, which regulates "collecting information from telecommunication networks". Pursuant to paragraph 3 of this Article, "collecting information from transport telecommunication networks shall consist in conducting with the use of appropriate technical means of surveillance, selection and recording of the content of information transmitted by a person and important for pre-trial investigation…". We consider the abovementioned provision to be sufficiently precise and foreseeable.

7.7.4.2 Authorization procedure

According to the case-law of the ECtHR, there are several factors which need to be taken into account in order to ensure that the authorisation procedures in domestic legislation are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration. These factors include, in particular, the authority competent to authorise the surveillance, its scope of review and the content of the interception authorisation.[219]

Pursuant to UaCPC, collection of information from transport telecommunication networks is **authorized by the investigating judge** (Article 263(2)). Moreover, these decisions fall under the competence of a limited number of courts, namely appellate courts within whose territorial jurisdiction the pre-trial investigation agency is located, or the High Anti-Corruption Court (Article 247(1)). This solution in itself provides for some protection against arbitrary application of the law.

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:

> *Article 250. Conducting a covert investigative (detective) action before investigating judge adopts a ruling*
>
> *1. In the exceptional and urgent cases related to saving human life and preventing the commission of grave or special grave crime as provided for by Sections I, II, VI, VII (Articles 201 and 209), IX, XIII, XIV, XV, XVII of the Special Part of the Criminal Code of Ukraine, a covert investigative (detective)*

[219] Zakharov v Russia, ECtHR app. no. 47143/06, para 257.

> *action may be initiated before investigating judge adopts a ruling in the cases prescribed by this Code, upon decision of investigator approved by the public prosecutor, or upon decision of the public prosecutor. In such a case, public prosecutor shall immediately after the initiation of such covert investigative (detective) action apply to investigating judge with an appropriate request.*
>
> *2. Investigating judge shall consider this request in accordance with the requirements of Article 248 hereof.*
>
> *3. Conducting any activities related to rendering a covert investigative (detective) action shall be immediately discontinued where 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 shall be subject to destruction as prescribed by Article 255 hereof.*

Urgent authorization procedure, as regulated in the UaCPC, seems to implement sufficient safeguards to protect against abuse of this procedural power. Most importantly, interception procedures which are initiated urgently and without authorization of the court must be immediately notified to the judge, and they undergo his *ex post* verification, which, in cases where judge rejects the interception order, should result in the destruction of obtained material.

Next, we look at the **judge's scope of review**. As explained in the introduction, the ECtHR has held that this authority 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.[220] The purpose of this is to ensure that "*secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration*".[221]

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". In general, this requirement indicates that assessment of necessity should be part of the judge's analysis. Moreover, 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, *inter alia*,

> *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 has committed it;*
>
> *8) information, depending on the type of covert investigative (detective) action, on identification signs, which will allow to uniquely identify the*

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

> *subscriber under surveillance, transport telecommunication network, and terminal equipment etc.;*
>
> *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 a request to authorize interception must contain all elements needed to establish (1) the existence of a reasonable suspicion against a person and (2) the necessity of conducting this action.

Nevertheless, it appears that judge's scope of review in relation to request for authorizing interception 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 per Article 248(3) a judge could authorize interception even when the prosecutor did not prove necessity, i.e., "impossibility to obtain otherwise knowledge on crime and the individual who committed it", nor the existence of reasonable suspicion about the person. 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".*

Hence, it appears that while the motion to authorize interception which is submitted to the court should contain all the necessary elements, the UaCPC does not oblige the court to consider those

elements, nor does it require that it provides reasons for its conclusions in relation to the abovementioned elements.

During the discussions already in 2018, 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.[222]

7.7.4.3 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". This provision is an important additional safeguard.

7.7.4.4 The duration of interception

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*".[223]

[222] 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.
[223] Zakharov v Russia, para 250.

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.*

Maximum duration of interception powers is set in relation to maximum duration of pre-trial investigation, which according to Article 219 of the UaCPC is twelve months in criminal proceedings in respect of minor crimes and eighteen months in criminal proceedings in respect of grave or special grave crimes. In our opinion, the conditions and safeguards mentioned above are sufficient to ensure protection against abuse.

7.7.4.5 Notification of interception of communications to the person concerned

As mentioned in the introduction, ECtHR consider that the notification of interception of communications "is inextricably linked to the effectiveness of remedies before the courts".[224] 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".[225] 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

[224] Zakharov v. Russia, para 286 and other cases quoted there.
[225] Zakharov v Russia, ECtHR app. no. 47143/06, para 287.

illusory rather than practical and effective. The national law thus eschewed an important safeguard against the improper use of special means of surveillance".[226]

In the legislation of Ukraine, notification of interception of communication to the person concerned is regulated in Article 253 of the UaCPC, which reads as follows:

> *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 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, procedures set in the abovementioned article are sufficient to ensure protection against abuse of the law. In particular, Ukrainian legislation prescribes the obligation to notify, and there is also a fixed deadline by which it must happen. In such circumstances, we consider that national legislation contains sufficient safeguards regarding notification requirements.

7.8 Oversight

It is very well established in the case-law of the ECtHR that due to the fact that surveillance of communications is exercised in secret, the risks of arbitrariness are evident.[227] It is therefore necessary that the state implements adequate safeguards against arbitrary application and abuse of the law. As explained by the ECtHR, "the overarching requirement is that a secret surveillance system must contain effective guarantees – especially review and oversight arrangements – which protect against the inherent risk of abuse and which keep the interference which such a system entails with the rights protected by Article 8 of the Convention to what is "necessary in a democratic society"".[228]

It appears appropriate to differentiate here between supervision in specific cases, described in the sections above, and systematic oversight of the operation of secret surveillance system as such.

In this context, the ECtHR has explained that the relevant factors for deciding whether the oversight arrangements are adequate are (a) the independence of the supervisory authorities, their competences, and their powers (both to access materials and to redress breaches, in

[226] Zakharov v Russia, ECtHR app. no. 47143/06, para 288.
[227] Zakharov v. Russia, paragraph 229.
[228] Ekimdzhiev and Others v. Bulgaria, paragraph 292.

particular order the destruction of surveillance materials), and (b) the possibility of effective public scrutiny of those authorities' work.[229]

The starting element here is that it appears that in Ukraine, like in many other countries, relevant authorities have direct access to networks of communication service providers and are in the position to execute surveillance without further technical or legal participation of those providers (see more extensively 7.7.1 above). In such circumstances, it is important to consider also the oversight of system as a whole.

Unfortunately, we have been able to identify only a limited number of provisions in the Ukrainian legislation relevant for this issue.

Starting point for the analysis here is the UaLSS contains several articles on the accountability and oversight of the Security Service of Ukraine. These read as follows:

> ***Article 31. Accountability of the Security Service of Ukraine***
>
> *Permanent control over the activities of the Security Service of Ukraine and its compliance with legislation is carried out by the Verkhovna Rada of Ukraine.*
>
> *The head of the Security Service of Ukraine annually, by February 1, submits a report on the activities of the Security Service of Ukraine to the Verkhovna Rada of Ukraine.*
>
> ***Article 32. Control of the President of Ukraine over the activities of the Security Service of Ukraine***
>
> *Control over the activities of the Security Service of Ukraine is carried out by the President of Ukraine and state bodies authorized by him.*
>
> *Permanent control over the observance of the constitutional rights of citizens and legislation in operational investigative activities and activities in the field of state secret protection of bodies and units of the Security Service of Ukraine, as well as control over the compliance of the provisions, orders, orders, instructions and instructions issued by the Security Service of Ukraine with the Constitution and laws of Ukraine is carried out by officials specially appointed by the President of Ukraine. The powers of these officials and the legal guarantees of their activities are determined by the Regulation, which is approved by the President of Ukraine.*
>
> *The Security Service of Ukraine regularly informs the President of Ukraine, members of the National Security Council of Ukraine and officials specially appointed by the President of Ukraine about the main issues of its activities, about cases of violations of legislation, and also submits other necessary information at their request.*
>
> *The head of the Security Service of Ukraine annually submits a written report on the activities of the Security Service of Ukraine to the President of Ukraine.*
>
> *The head of the Security Service of Ukraine bears personal responsibility for the timeliness, objectivity and completeness of the submitted information.*

[229] Ekimdzhiev and Others v. Bulgaria, paragraph 292 et seq.

Regarding the parliamentary control, we have been able to identify some provisions in the Chapter 38 of the Regulations of the Verkhovna Rada of Ukraine (UaRVR), but in essence these contain only rules regulating the consideration of Service's annual report. Likewise, we also revied provisions of the Law on committees of the Verkhovna Rada of Ukraine, but we did not identify provisions which would specifically regulate the oversight over the Service in its surveillance activities.

When it comes to the presidential control, there is an appointed Commissioner of the President of Ukraine for control over the activities of the Security Service of Ukraine.[230] However, we have not been able to identify provisions regulating the powers and competences of the Commissioner.

In such circumstances, it is not possible to give objective assessment on the state of oversight in Ukraine. However, under the premise that there are no other sources of law regulating this issue, than oversight as it is currently regulated would be falling short of the relevant European standards.

7.9 Summary and recommendations

- It appears that there is sufficiently clear distinction of powers between UaCPC and the UaLOIA.
- UaCPC prescribes reasonably foreseeably that electronic evidence can be used in criminal proceedings.
- Ukrainian legislation does not differentiate properly between various categories of data which are recognized by the Convention. To be sure, procedural powers in the UaCPC in general cover all categories of data which are recognized by the Convention. But for instance, it is not precisely defined in the legislation which exact categories of data are subject to powers implementing monitoring of traffic data or acquisition of subscriber information. The notion of subscriber information is not adequately regulated in the law.
- Expedited preservation of stored computer data and preservation and partial disclosure of traffic data are not regulated as standalone procedural powers. It is recommended that this be rectified, since these powers would additionally empower Ukrainian law enforcement authorities and at the same time would contribute to proper execution of procedural powers, in line with Article 15 of the Convention.
- Production order seems to be well regulated in the UaCPC. Although there are no specific rules for production of subscriber information, general rules are broad enough in order to be applicable to this case as well. Also, Article 15 safeguards seem to be well applied.
- There have been no substantive changes in the regulation of search and seizure compared to the last assessment. Most important conditions and safeguards seem to be implemented. There are no specific rules pertaining to extended search as regulated in the Article 19(2) of the Convention.
- Ukraine implements Articles 19 and 20 of the Convention in most parts. Major conditions and safeguards are found in the Ukrainian legislation. Still there is some

[230] https://zakon.rada.gov.ua/laws/show/en/744/2019#Text

room for improvement, in particular regarding necessity testing and ensuring that these powers are applied only in cases when there is no alternative. Also, we have not been able to identify system of oversight over application of secret surveillance measures which would be in line with European standards.

8 Executive summary and recommendations

In this section we summarize the main findings and general recommendations of this report.

- While it is not directly relevant for the subject matter of this report, it is important to note and recognize that most of the analysed countries made significant progress in the digitalization and organization of national legislation. National legislative portals are nowadays offering open access to up-to-date consolidated versions of the relevant laws, which significantly improves the ability of citizens and business actors to understand the law and act in accordance with it. Also, some countries (Georgia, Ukraine) also offer official translations of most important national acts which greatly improves the possibilities of analysing national law from the comparative perspective.

- Legal systems of all analysed countries prescribe procedural powers, in addition to criminal procedure codes, also in laws on operative-intelligence activities. These are laws which pursue much broader mandate than criminal procedure codes and typically empower multiple national authorities (i.e., in the national security, financial, customs, border control and other areas) to execute procedural powers defined therein. Some countries (Georgia, Moldova, Ukraine) are prescribing relatively clearly that procedural powers defined in those laws must be executed also in line with the requirements of the criminal procedure codes. For Armenia the situation seems to be vague since national legislation is not completely precise in this context. Azerbaijan and Belarus seem not to draw a clear line between these laws when they are used to investigate and prosecute criminal offences. Moreover, many important safeguards are missing in these laws. Likewise, for the purposes of this report we analysed those laws just from the perspective of the Convention. But in reality, their application is much broader and can lead to interferences with private life in many different domains. In this context, it is important to note that the ECtHR had the opportunity to analyse similar legislation in the case of *Zakharov v. Russia* and found it lacking in many aspects. We are concerned that similar conclusions might be made also in relation to laws of countries mentioned in this report. Therefore, looking broadly, it seems to be very important to put these laws into focus and attempt to bring them in compliance with relevant European standards.

- Criminal procedure codes of all analysed countries prescribe in a reasonably clear and foreseeable manner that electronic evidence is acceptable in criminal proceedings. In all countries this is done using the traditional concept of "document" as one of the sources of evidence, with additional stipulations in the laws that this notion includes data in various data carriers, including electronic. In the absence of information from the case-law to the contrary we consider that these definitions are acceptable from the perspective of human rights requirements.

- As explained in the introduction, procedural powers in the Convention are built in relation to specific categories of computer data. Georgian and Moldovan legislation properly defines categories of computer data and prescribes procedural powers relevant for these categories. On the other hand, majority of countries (Armenia, Azerbaijan, Belarus) do not differentiate properly between various categories of data (computer data in general, traffic data, subscriber information, content data). In Ukraine there is some distinction between these concepts, but the issue is that they

are mostly left undefined, which reduces foreseeability of legislation. It seems necessary to undertake additional efforts to improve national laws in this regard. This is particularly important for the compliance with Article 15 of the Convention as well, because there can be no true application of the principle of proportionality by the law enforcement authorities if they do not have at their disposal all the necessary procedural tools. Also, requirements of precision and foreseeability of legislation mean that citizens and data holders should have appropriate understanding which categories of data can be accessed on the basis of relevant procedural powers. In order to enable this, it would be necessary to define those categories in the legislation with sufficient precision.

- Most analysed countries still do not implement expedited preservation of stored computer data as a standalone procedural power. Except for Moldova, countries rely on production orders or search and seizure power to ensure urgent preservation of data. This significantly reduces the ability of national law enforcement authorities to utilize less intrusive powers instead of more serious ones. Also, such an approach might disproportionately affect the interest of legitimate data holders such as service providers, who should be 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. In the absence of legally defined preservation requests service providers and other business data holders might eventually decide to cooperate with the authorities voluntarily, based on informal requests. While this might serve the needs of law enforcement authorities in some circumstances, it creates legal issues for such data holders, since they are under the pressure from personal data protection and other laws to share personal data of their users only when clear legislative grounds for that exist. Also, domestic authorities will presumably have more success with outgoing requests for international assistance in matters of data preservation if they can point to specific provisions in domestic legislation. Hence, it is recommended that additional efforts be undertaken to ensure that all analysed countries properly implement preservation orders as standalone procedural powers.

- Power of expedited preservation and partial disclosure of traffic data is not regulated in the laws of Armenia, Belarus, Azerbaijan, Georgia and Ukraine. Moldovan legislation implements provisions on expedited preservation of traffic data and their partial disclosure, which are mostly in line with the Convention. As above, this is an issue which should be addressed by national legislators. In particular, capacity of countries to engage fully in data exchanges on the basis of Convention's rules on international cooperation might be improved by the implementation of Article 17.

- Rules on search and seizure are present in all analysed countries. In Armenia the new CPC regulates so-called digital search and there are specific provisions on seizing computer data. Most important conditions and safeguards are implemented. In Azerbaijan situation remained mostly unchanged compared to previous assessment. There is need to address implementation of Article 19(2,3) of the Convention, as well as to develop some missing safeguards. Belarus improved its legislation by adding new rules on seizure of stored computer data, which is a welcome development. Nevertheless, there seem to exist substantial issues when it comes to conditions and safeguards, the most important of which is the questionable practice of giving authorizations by prosecutors. Moldovan and Georgian legislation is mostly in line with

the Convention, with some room for improvement in both cases. The same is applicable for Ukraine as well.

- When it comes to secret surveillance powers, most countries also implement rules on real-time collection of traffic data, either as standalone powers such as in Moldova and Georgia, or as part of general powers to interfere in private communications. Likewise, for interception of content, there are legal grounds in place, but when it comes to conditions and safeguards countries pursue many different approaches. Belarus unfortunately fails to implement majority of necessary safeguards. Some serious limitations can be identified in legislation of Azerbaijan, and to lesser extent in Ukraine and Armenia. Moldova and Georgia seem to have improved their legislations in this context significantly.

- In most countries, the most pressing issue appears to be oversight of secret surveillance systems. Namely, while there are some effective safeguards in the context of individual proceedings, when we look at the system as a whole, the situation appears more pessimistic. The main issue here is that all countries seem to implement systems in which communication service provides enable law enforcement authorities to execute direct access to their systems. Also, it appears that in all countries' entities in the domain of national security and intelligence are technically in position to execute surveillance orders. While this is not problematic *per se*, it does call for a very strong and effective oversight arrangements. Unfortunately, we did not identify such arrangements in countries analysed in this report. Even in the country which has the most developed legislation in this context- Georgia – legislation falls much below the relevant European standards. Hence, this issue might be treated as a priority in future legislative activities, both by countries themselves and through assistance of the Council of Europe.