Cybercrime@EAP III

Public/Private Cooperation under the Partnership for Good Governance with Eastern Partnership countries

2016/DGI/JP/3608
28 May 2017

Suggestions for draft amendments to procedural legislation of Armenia concerning cybercrime and electronic evidence

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

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

This review has been prepared by independent Council of Europe experts Catherine Smith, Marko Juric and Zahid Jamil with the support of the Cybercrime Programme Office of the Council of Europe.

This document was produced with the financial assistance of the European Union. The views expressed herein do not necessarily reflect positions of the European Union or the Council of Europe.

Contact: Cybercrime Programme Office of the Council of Europe, Bucharest Romania. Email: cybercrime@coe.int

1 Background

The European Union and the Council of Europe supported Eastern Partnership countries between 2011 and 2014 through the Cybercrime@EAP I project. Two follow up projects, Cybercrime@EAP II and Cybercrime @EAP III, were launched, in May and December 2015 respectively, with focus on international cooperation and public-private partnerships in cybercrime and electronic evidence. All countries – with the exception of Belarus – are Parties to the Budapest Convention on Cybercrime and are thus members of the Cybercrime Convention Committee (T-CY).

During Cybercrime@EAP I, Eastern Partnership countries concluded that public/private cooperation, in particular with regard to access to electronic evidence for criminal justice purposes, was a strategic priority. This was reconfirmed during the launching event of the Cybercrime@EAP II project in September 2015. Throughout discussions at the Regional meetings of the Cybercrime@EAP II project in Tbilisi (14-16 December 2015) and Kyiv (4-5 April 2016), the importance of proper legislative background for international cooperation on cybercrime and electronic evidence was repeatedly highlighted.

Armenia has indicated, throughout these meetings and in-country events (in particular, the Workshop on International Cooperation held in Yerevan on 15-17 June 2016 under the Cybercrime@EAP II project) that the new Code of Criminal Procedure was in the final stages of development, which should reportedly remedy all of the outstanding issues of compliance of Armenian laws with the Budapest Convention on Cybercrime. In this respect, the expertise of the Council of Europe in providing a balanced approach between the efficiency of criminal investigations, access to electronic evidence and relevant safeguards and guarantees, can provide an important contribution toward reforms initiated by Armenia in this regard.

To address the above-mentioned problems, in the framework of the Cybercrime@EAP III project, the Cybercrime Programme Office has contracted the Council of Europe experts, Ms Catherine Smith from Australia, Mr Marko Juric from Croatia and Mr Zahid Jamil from Pakistan, to provide a review of the draft Code of Criminal Procedure of Armenia in terms of compliance with the Council of Europe Convention on Cybercrime and other applicable standards. The discussion with Armenian counterparts on 3-5 May 2017 in Yerevan, organized under the Cybercrime@EAP III project, allowed experts to discuss the details of the draft and suggest some recommendations for further improvement, which are outlined in relative detail in the current report.

2 Recommendations proposed by the experts

2.1 Definition of electronic evidence

2.1.1 Recognition of electronic evidence

There is no specific recognition of electronic evidence in the draft Code. Article 6, sub-article 36 defines the term evidence as "data about a fact, which is received in accordance with the procedure provided by law." The context in which the term "data" has been used in other provisions in the Code such as Article 87 and Article 88, suggests that the term may refer to physical carriers of information and not electronic data. Thus, there is ambiguity on whether the definition of evidence includes electronic evidence.

Article 86 provides a list of types of evidence in Criminal Proceedings, which does not specifically include electronic evidence. Article 86 includes "Off-proceedings documents", which term has been defined under Article 96 as "any record made on a paper, magnetic, electronic, or other medium in the form of words, numbers, sketches, or other signs, which contains data on facts that are

significant for the Criminal Proceedings, and was created outside the scope of the particular Criminal Proceedings."

Thus, the recognition of electronic off-proceedings documents may, to certain extent, be used to address the challenges resulting from the general non-recognition of electronic evidence. However, off-proceedings documents are limited to documents created outside the scope of particular criminal proceedings as a result of covert intelligence operations, and do not include electronic documents obtained as a result of exercise of powers by law enforcement with respect to a specific investigation. Evidence in electronic form is thus only recognized under the Code to the extent that such evidence has been obtained by intelligence operatives.

This shortcoming may be addressed by introducing the concept of "electronic evidence" in the list of types of evidence in Article 86.

2.1.2 Provisions related to evidence not applicable to electronic format

Certain provisions in the Code have been drafted for applicability to evidence in physical form, and may not be suitable for electronic evidence.

Article 21, sub-article 4 provides that a "Judicial Act may be based only on such Evidence during the examination of which equal conditions were safeguarded for each of the Parties". While this provision may be suitable for evidence in physical form where the accused may be presented with the opportunity to examine the original evidence, it may not be suitable for electronic evidence where it may not be possible to make the original evidence available to the defence. Thus, this may present the defence with the opportunity to invalidate all electronic evidence where they have not had an opportunity to examine such electronic evidence in its original form.

Article 22 provides that "Every factual circumstance constituting a part of the Accusation shall be substantiated with such volume of Evidence that will preclude any reasonable suspicion regarding such circumstance being proven." Given that the term "Evidence" does not specifically include evidence in electronic form, Article 22 may have the effect of requiring the Accusation Party to, prior to proving the contents of electronic evidence, having to prove the vessel of such evidence. This would have the result of placing an additional burden of proof on the Accusation Party in proceedings primarily based on electronic evidence.

Recommendations:

1. Introduce sub-paragraph 11 to Article 86, paragraph 1:
"Article 86. Types of Evidence
1. The following is Evidence in the Criminal Proceedings:
…
11) Electronic Evidence."

2. Adjust the definition of evidence in Article 6 to refer to electronic evidence:
"Article 6. Definitions of Key Terms Used in This Code
As used in this Code, the terms below shall have the following meaning:
…
39. Evidence: data about a fact, *whether in physical or electronic form,* which is received in accordance with the procedure provided by law, and based on which an Investigator, a Prosecutor, or a Court determine the existence or absence of circumstances subject to proving, as well as other circumstances significant to the proceedings."

2.2 Admissibility and chain of custody

The general rules of admissibility in the Code apply generally to all kinds of evidence, and given that there is no specific recognition of electronic evidence in the Code, there are no specific provisions with respect to admissibility of electronic evidence. While separate rules for admissibility of electronic evidence is not a requirement from a perspective of law and practice under the Budapest Convention, certain qualities of electronic evidence may require a careful review of applicable rules of evidence.

Chapter 11 provides certain measures for the safeguarding and disposition of evidence. Article 98 requires that "Physical Evidence shall be kept with the materials of the proceedings until the issue of their custody has been solved by a Conclusive Procedural Act". This condition may not be appropriate for electronic evidence given that electronic evidence is often stored on servers or remote storage and may not always be physically kept with the materials of the proceedings.

The Code does not provide appropriate safeguards for handling electronic evidence including mechanisms and procedures for ensuring chain of custody or integrity of electronic evidence. The drafters are thus invited to consider more specific rules keeping in view the current version of the Council of Europe Electronic Evidence Guide.

Article 97, sub-article 2 provides that any "Data obtained with a material violation of the law….shall be recognized as impermissible and may not be used as Evidence". Article 97, sub-article (3) lists conditions that result in data being obtained in material violation of the law. A new paragraph may be inserted thereunder providing that where the chain of custody or integrity of the evidence has not been maintained, such evidence shall be deemed to be obtained with a material violation of the law.

Recommendation:

Introduce sub-paragraph 8 under Article 97, paragraph 3:

"**Article 97. Evidence Permissibility and Restrictions of Its Use**
…
3. Data shall be deemed to have been obtained with a material violation of the law, if it was obtained:
…
(8) Where the chain of custody of the evidence has not been maintained, or where the integrity of the evidence has been compromised."

2.3 Definitions of categories of data

The Code does not specifically provide for different categories of data, including subscriber information, traffic data and content data. Only Article 249 provides some reference to some of these concepts, but in a manner that limits their application to only covert investigative actions; some elements of these definitions are missing as well.

2.3.1 Limited applicability of notions of subscriber information, traffic data and content data

The scope of Article 249 is limited to monitoring or "*secret collection and storage of data*" and it does not specifically extend to procedural powers under Article 16 (Expedited preservation of stored computer data), Article 17 (Expedited preservation and partial disclosure of traffic data),

Article 18 (Production orders) and Article 19 (Search and seizure of stored computer data) of the Budapest Convention.

Thus, the Code only recognizes the elements of some categories of data (content data, traffic data and subscriber information) to the extent of monitoring under Article 249, but not for other procedural powers under the Code, including demand for information under Article 239 and taking documents or objects under Article 240 (meant to enforce production orders).

2.3.2 Conflation of traffic data and subscriber information

Article 249 of the draft Code recognizes two kinds of data relating to internet communications: (1) "the contents of the communication"; and (2) "the geographic location, day, time, and duration of entering and exiting the Internet, the Internet user's or subscriber's name and user ID, the telephone number used to connect to the common telephone network, the Internet address, including the Internet Protocol (IP) address, the name of the Internet telephone call recipient and his personal identification data."

Thus, whereas Article 249 recognizes the distinction between content data and traffic data/subscriber information, it conflates the notions of traffic data and subscriber information. Resultantly, the Code does not address varying safeguards for different procedural powers, including separate grounds, thresholds and mechanisms to implement safeguards for collecting and storing subscriber information and traffic data.

The distinction between content data, traffic data and subscriber information should thus not be only formal, but also functional in terms of procedural powers and safeguards. It is not necessary that the same degree of independent supervision is required to seek ordering of subscriber information, as would be for ordering the real-time collection of traffic data.

2.3.3 Related concept of service providers

Some of the procedural powers required by the Cybercrime Convention apply only to the communications service providers. While it is up to the authorities of a specific country to decide whether this concept is used only for the purposes of criminal procedure or general definitions in specialized electronic communications legislation can be used, the existence of the notion of service provider distinct from other addressees of relevant procedural powers is important for the purposes of compliance with the Budapest Convention.

Recommendations:

1. Article 6 of the draft Code can be amended to introduce relevant definitions of three categories of data:

*"**Subscriber information** - information aimed to identify the subscriber to the communications service, which can establish the type of communication service used, the technical provisions taken thereto and the period of service, the subscriber's identity, postal or geographic address, telephone and other access number including IP address, billing and payment information, and any other information on the site of the installation of communication equipment, including information available on the basis of the service agreement or arrangement;*
***Traffic data** - 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 (traffic data);*
***Content data**: Data relating to the meaning or purport of the communication, or the message or information being conveyed by the communication."*

2. Update Article 249 of the draft Code to reflect the moving of definitions of traffic and content data to general provisions of Article 6; in particular, simplify the wording of par. 2(2) and 3(3) of the Article 249 (please refer below to the section related to real-time collection of traffic data).

3. Consider introducing the concept of a "service provider" under specialized legislation and/or criminal procedure, in line with the definition provided by the Budapest Convention on Cybercrime:

"***Service provider*** *- Any state or local government entity or private entity that provides to users of its service the ability to communicate by means of a computer system, and other entity that processes or stores computer data on behalf of such communication service or users of such service*."

2.4 Expedited preservation and provisional disclosure of stored computer data

Expedited preservation of stored computer data (Article 16 of the Budapest Convention) is a measure which can be used to secure (existing) computer data, where there are grounds to believe that it is vulnerable to loss or modification. This measure is provisional, meaning that it is only a first step in the process. Once the data is secured, preservation may (or may not) be followed by other measures which are aimed at actually obtaining it. In essence, the whole purpose of expedited preservation is to secure data before actually obtaining it.

Pursuant to the Article 16 of the Convention, its Explanatory report, as well as reports adopted by the Cybercrime Convention Committee (T-CY), there are essentially two methods of ensuring compliance with Article 16. The first is for a Party to introduce specific preservation order in its domestic legislation, and the alternative is to use production order or search and seizure mechanism to expeditiously gain possession of data. Although both approaches can be valid under the Convention, the first (standalone preservation order) is considered more appropriate. By introducing such preservation order in its legislation, State provides for a greater flexibility in the application of the law, and at the same time enables its law enforcement authorities to initially use less-restrictive measure (preservation) instead of more coercive ones (production or seizure).

Article 17 of the Convention creates additional procedural powers when preservation of traffic data is necessary. In essence, Party must 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". In particular regarding the second requirement, Party must ensure that national authorities can order one service provider to expeditiously disclose those traffic data which are necessary to identify the next provider in communication chain, so that preservation notices can be served further.

Current draft Criminal Procedure Code of Armenia does not contain provisions implementing Articles 16 and 17 of the Cybercrime Convention as a standalone measures. Therefore, it is necessary to analyse whether the purpose of these provisions can be achieved by the application of some other procedural powers in the draft CPC.

Firstly, it might be possible to argue that Article 232 (Demand for information) might be applied as a method of production order, thereby enabling expedited preservation of data. However, there are several shortcomings here. To begin, this measure cannot be applied against natural persons (Article 232 addresses "state or local government bodies, legal entities, or any organization…"). Moreover, it is not clear whether this article can be applied to computer data. While it is possible to argue that the notion of "information" is broad enough to include computer data, such outcome

would nevertheless depends on the readiness of the courts to give necessary meaning to this notion. Finally, the meaning of the exception stipulated in paragraph 2, second part ("or when certain documents, objects, or other materials are demanded") is not precise, and this might also have impact on the application of this provision. In such circumstances, we conclude that the purpose of Article 16 of the Convention cannot be achieved by applying demand for information measure.

Secondly, "Taking Documents or Objects" (Article 233) could not be applied to the present situation, since it implies access to documents or objects "which have been presented by any person". Literal meaning of this provision suggests that initiative to present documents or objects must come from a third person and not from the LEA. Consequently, this provision is not sufficient to give full effect to the Article 16 of the Convention.

Thirdly, general search and seizure (Article 235 et seq.) powers might also be relevant. As noted above, this approach could still be valid under the Convention. But, taking into account the fact that certain searches can be made only with the court warrant (see in particular CPC 298 et seq. ("Scope of the Judicial Safeguards of the Performance of Proving Actions") and in accordance with strict procedural conditions and safeguards, the main concern is that search and seizure may not be applied expeditiously enough in order to give full effect to Article 16 of the Convention.

Finally, CPC does not contain any provision implementing Article 17 of the Convention. In terms of very specific and technical powers regarding preservation and partial disclosure of traffic data by the service providers, implementation on the basis of expedited application of traditional powers (production, search and seizure) may not seem possible; specific legal provision to this effect in the draft CPC would be most advisable.

Recommendations:

In order to ensure full compliance with Articles 16 and 17 when introducing a standalone preservation order, drafters of the CPC should take into account the following:

1. Preservation order should be applicable for any computer data, including traffic data, content data and subscriber information. These notions should be defined in line with the Convention;
2. Preservation order should be applicable against any legal or natural person who possesses or controls data. It is mandatory that scope of application of such order includes service providers, but is not limited to them. However, service providers should be subject to an additional obligation: to disclose upon request amount of traffic data sufficient to identify the next provider in the communication chain. This is necessary to give effect to Convention's Article 17;
3. Preservation order should be applicable in criminal proceedings regarding any type of crime;
4. It should have limited duration, that is, "for a period of time as long as necessary, up to a maximum of ninety days". However, competent authorities may be allowed to renew the order if necessary;
5. There should exist possibility of obliging "the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by domestic law";
6. Preservation order should be understood to be limited to existing data (data already stored on a computer system). In other words, Article 16, unlike laws about data retention, does not call for preservation of data which might come into existence in the future.

As regards conditions and safeguard applicable to preservation order, it was noted by the Cybercrime Convention Committee that those should not be too restrictive or complex, so that it is possible to ensure preservation in an expedited manner. In this context, the following should be taken into account:

- National legislation should observe general principles regarding quality of the law. This includes, in particular, requirement that legal provisions be clear, precise and foreseeable;
- Judicial oversight over the issuing of preservation order is not necessary, since such measure interferes only in the slightest possible manner with the interests of person who is required to preserve data. Consequently, preservation orders can be issued by investigators and/or prosecutors.

In order to give effect to Articles 16 and 17 of the Convention, new Article can be added to the draft Code, with the following text:

"***Article 232[1]. Expedited preservation of stored computer data and provisional disclosure of traffic data***

1. Where there are grounds to believe that stored computer data can be lost or modified, the investigator can issue a ruling obliging any natural or legal person in whose possession or under whose control such data is reasonably believed to be located, or any service provider involved in a chain of communication, to preserve specified computer data and maintain its integrity for a period of 90 days. This term can be extended to another 90 days, where necessary.
2. For the purposes of this Article, stored computer data means any information contained in the form of computer data or any other form. This includes, but is not limited to:
- information aimed to identify the subscriber to the communications service, which can establish the type of communication service used, the technical provisions taken thereto and the period of service, the subscriber's identity, postal or geographic address, telephone and other access number including IP address, billing and payment information, and any other information on the site of the installation of communication equipment, including information available on the basis of the service agreement or arrangement (subscriber information);
- 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 (traffic data);
- content of the communication.
3. The ruling of data preservation shall stipulate the obligation of the custodian of the preserved computer data to keep confidential the undertaking of such procedures for the period of time referred to in par. 1 of this Article.
4. The ruling of data preservation, where necessary, shall oblige a service provider to immediately disclose sufficient amount of traffic data to requesting investigator/prosecutor to enable the investigation to identify the service providers and the path through which the communication was transmitted."

2.5 Production Order

In order to properly implement Article 18 of the Convention, Parties should adopt legislative and other measures necessary to order any person to order

- a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
- a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Parties should take into account the following when implementing Article 18:

Purpose of production order: to obtain computer data by less intrusive means than seizure. As was elaborated in Explanatory report, "a "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control…".

Object: any computer data, including subscriber information, which is possession or control of a person against whom the order is directed. Being limited to existing computer data, Article 18 does not create obligation to retain data or keep any sort of records.

Subject: any natural or legal person, including service providers.

Relevancy: Subscriber information is the most often sought category of data in domestic investigations but also at the international level. Ability to obtain such information is indispensable for successful investigation and prosecution of cybercrime.

When it comes to the draft Code of Criminal Procedure of Armenia, Article 232 of the draft Code lays very basic groundwork with respect to production orders. However, Article 232 is missing several key elements of this procedural power, as required under Article 18 of the Budapest Convention:

2.5.1 Scope of Article 232 with regard to computer data

The scope of Article 232 has not been clearly defined. Article 232 relates to the power of the investigator to demand "information". The Code does not provide any definition of the term "information" and thus it is unclear whether Article 232 enables the investigator to demand the production of computer data.

Certain language within Article 232 itself suggests that this procedural power is not intended to be exercised with respect to computer data, namely, par. 3 provides that: "The requested information shall be provided … in the form of a statement, which shall be annexed to the Protocol of the demand for information." Given that the manner prescribed in Article 232 for production of information is only appropriate for physical information, it appears that this provision does not currently extend to computer data.

2.5.2 Subject of production orders

The power of investigators under Article 232 permits making a demand for information to "state or local government bodies, legal entities, or any organization possessing information about circumstances of significance to the proceedings." Article 232 thus does not authorize an investigator to make a demand from natural persons in possession of information, contrary to the requirements of the Article 18 of the Budapest Convention.

Article 232 requires that the subject of a production order to have information in its possession, but does not apply where such information is in control of the subject and not in its possession. Thus, Article 232 would have limited effect in enabling investigators to seek production of data under control of the subject. Due to this limitation, the investigator under Article 232, for example, will be unable to demand production of cloud data that is stored on a third-party cloud service operating outside Armenia, even if state or local government bodies, legal entities, or an organization in Armenia is in control of such information.

2.5.3 Applicable conditions and safeguards

National legislation should observe general principles regarding quality of the law. It might exclude privileged data or information from the scope of production order. There is no universal requirement that judicial authorization is required to order production of data. As elaborated in the Explanatory report to the Budapest Convention: "with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required". At least for subscriber information, many countries allow that such information can be obtained through a formal police request or an order of a prosecutor. On the other hand, higher standards should be applied to order production of content data.

In contrast, Article 232 of the draft CPC does not provide for any procedural safeguards with respect to the exercise of the power of demand for information. The investigator is not required to seek prior permission from a judiciary officer, thus there is no requirement for any independent supervision with respect to the exercise of this power. In order to satisfy the requirements of Article 15 of the Budapest Convention, such authorization in respect of at least traffic and content data needs to be introduced.

2.5.4 Absence of extraterritorial application of production orders

Article 232 does not provide investigators with the power to specifically order production of subscriber information from service providers offering services in Armenia, including from service providers that are not located in Armenia but that have such subscriber information in their control or possession, as provided under Article 18.1.b. of the Budapest Convention. The scope of the procedural power is thus limited and does not necessarily enable investigators to order service providers located outside Armenia, but offering services in Armenia, to produce subscriber information.

Recommendation:

Make the following adjustments to the current draft of Article 232 of the Code:

"**Article 232. Demand for Information**
1. A demand for information is an Investigator's written application to *any person*, state or local government bodies, legal entities or any organization possessing *or having control over* information about circumstances of significance to the proceedings. *Demand for information can be served on a service provider offering its services in the territory of Armenia, requesting subscriber information relating to such services in that service provider's possession or control.*
2. A demand for information shall be binding for its addressee, with the exception of cases in which the demanded information is a secret protected by law, or when certain documents, objects, or other materials are demanded. *Traffic and content data requested under this Article can be provided to the investigative authority on the basis of the court decision.*
3. The requested information shall be provided during the time period set by the Investigator *in any manner specified in the written application.*"

2.6 Search and Seizure

Article 19 of the Cybercrime Convention (the Convention) requires that every Party adopts legislative and other measures as may be necessary to empower its competent authorities to search or gain access within their territory to:

a. computer system or part of it and computer data stored therein; and
b. a computer-data storage medium in which computer data may be stored.

Article 19 of the Convention provides a contemporary approach for the search and seizure of computer data. When a provision is enacted into national law, the purpose of the provision should be to enable access to computer data in a way that does not reduce the integrity of the evidence. As such, it is important to modernise search and seizure provisions so that they can adapt to the dynamic nature of electronic evidence.

One of the major challenges to law enforcement agencies is the dynamic and transnational nature of cybercrime. It is essential that agencies can search and seize information in electronic format before it is destroyed, encrypted, or moved outside state territory. Laws that do not meet the necessary requirements will restrict the ability of competent authorities to obtain digital evidentiary material.

The draft Criminal Procedure Code of Armenia appears to be restrictive in the approach to the search and seizure of computer data. The language used in the relevant provisions at relating to search and seziure appear to relate to physical search of objects. As an alternative, Article 226 ("Inspection") in its par. 3 acknowledges that technical means may be used for "observation", but this language may be limiting when the investigator needs to access a computer system and, moreover, seize the information in question.

Moreover, Article 19(2) of the Convention provides the framework for agencies to extend their search beyond the computer which may be subject to the initial search. This envisages situations where information is remotely accessible (within same territory), on a computer that is connected and where the investigator is satisfied that the information on that computer is related to the search being undertaken. The relevant provision requires elaboration to include access to connected computers and to ensure that the power is available for ongoing criminal investigations. This power should be subject to the applicable safeguards and guarantees relevant in the context of search.

Article 19(3) of the Convention is significant as it envisages circumstances where it may not be possible to make a copy and it is necessary to seize or similarly secure a computer system. The concept of rendering computer data inaccessible is a significant power that should be addressed. Rendering computer data as inaccessible deprives the target from having access to the data during the criminal proceedings. The type of data that Article 19 envisages is data that may be illegal, destructive or can do social harm. The Convention's language of "seize or similarly secure", addresses more than one investigation scenario, it provides for the collection of evidence by copying and provides for evidence to be confiscated or made inaccessible by the owner of the data. Having these powers in domestic law will also enable effective collection of electronic evidence and where necessary provide for forensic examination by specialists.

Article 226 of the draft CPC on "Inspection", as noted above, attempts to specifically address the inspection of computer software and appears to provide for a computer to be secured; however, the language of the provision would still be lacking to cover all the objectives of Article 19(3) of the Convention, such as:

a. seize or similarly secure a computer system;.
b. make and retain a copy of those computer data;
c. maintain the integrity of the relevant stored computer data; and
d. render inaccessible or remove those computer data in the accessed computer.

Taking into account the above arguments, it is preferable that more substantive adjustments are made to the search and seizure provisions of the draft Code (Articles 236 and 239) rather than focusing on updating and refining "inspection" as the power implementing the relevant requirements of Article 19 of the Convention.

Recommendation:

Due to the complexity of obtaining evidence by electronic means, the draft CPC should be amended, refined, and strengthened to ensure that there is no doubt that computer data obtained under the search, or seized under warrant is collected in a manner that can be later admitted into evidence. The language of Article 19 of the Convention should be reviewed and used as the basis to amend the draft CPC. By amending the CPC to address the issues noted above, the relevant amendments will provide for effective computer data search and seizure provisions that are consistent with the Convention.

The following changes may provide useful guidance in this respect:

"**Article 236. Procedure of Performing a Search**
1. The Investigator and the persons participating in the investigative action shall, based on the decision on performing a search, enter the building or site where the search is to be performed.
2. Prior to performing the search, the Investigator shall be obliged to familiarize the person, in whose premises the search is being performed, with the decision and deliver a copy of the decision to him. His signature about it shall be taken.
3. After delivering a copy of the search decision and publishing the decision, the Investigator shall offer to present the searched objects or the Accused who is hiding. If they are presented voluntarily, then the searching actions shall not be performed. Otherwise, the search shall continue.
4. When performing a search, the Investigator shall have the right to open closed Houses, buildings, and storages, if the person concerned refuses to open them voluntarily. The Investigator shall take measures to preclude or minimize potential damage to locks, doors, and other objects. *If, during the search, the investigator performs search or similarly accesses specific computer system or part of it and has grounds to believe that the data sought is stored in another computer system or part of it is in on the territory of Armenia and such data is lawfully accessible from or available to the initial system, the investigator shall be able to expeditiously extend the search or similar accessing to the other system.*
5. In addition to what is specified in the search decision, the Investigator shall also take all the objects discovered during the search, which by law are taken out of circulation or, in terms of their nature, differentiating marks, or traces thereon, may be linked with another alleged crime.
6. All actions of the person performing a search shall be visible to those present during the search.
7. The Investigator may prohibit the persons present at the search site to leave such site or to communicate with one another and other persons until the search is over.
8. All objects taken shall be presented to the participants of the investigative action and, if necessary, packaged and sealed with the Investigator's seal.
9. Persons who are present at the search may be required to disclose their knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in the above paragraphs."

"**Article 239. Seizure**
1. Seizure is the taking of certain objects, materials, or documents upon the Investigator's initiative, which are of significance to the proceedings and are located in a definitely known place or are held by a specific person.
2. Objects in a House, as well as documents or objects containing banking secrets, notary secrets, insurance secrets, and securities market service secrets may be seized only if an appropriate Court decision is present.
3. Documents containing state secrets may be seized only with the Prosecutor's permission, in a procedure agreed upon with the head of the respective state body.

4. Documents or objects containing banking or adjacent secrets may be seized only in those cases when they relate to the Accused or the legal person in connection with which there is a reasonable assumption, that its activity as a whole or as a part, are controlled or otherwise guided by the Accused.
5. In case of performing seizure by an Investigator's decision, the decision shall contain a brief overview of the alleged crime in respect of which the performance of the seizure is necessary, as well as the object to be seized and the time and place of performing the seizure.
6. Based on the decision to seize, the Investigator and the persons participating in the investigative action shall enter into the building or site where the seizure is to be performed. *Where electronic evidence is to be seized, the relevant decision on seizure should specify if the seizure of the data carrying device is necessary or if a copy of the data will be sufficient, including the following options:*

- *seize or similarly secure 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.*

7. Before making the seizure, the Investigator shall be obliged to familiarize the person, in whose premises the seizure is made, with the decision and to deliver a copy of the decision to him. His signature about such fact shall be taken.
8. After delivering a copy of the seizure decision and publishing the decision, the Investigator shall offer to present the object subject to seizure. In case of failing to present documents or objects containing notary, banking or adjacent secrets, the Investigator shall have the power to perform searching actions for the purpose of discovering them. In other cases, the performance of searching actions on the basis of a seizure decision shall be prohibited.
9. If the object or document subject to seizure is in the materials of other criminal, judicial, or administrative proceedings, then a photo of the object or a copy of the document, signed by the person conducting the proceedings, shall be given to the Investigator. The original of the object or document may be given to the Investigator only for the purpose of performing an expert examination.
10. All seized objects shall be presented to the participants in the investigative action, described in detail in the Protocol and, if necessary, packaged and sealed with the Investigator's seal.
11. A copy of the seizure Protocol shall be delivered to the person in whose premises seizure was made or to an adult member of his family, against their signature. If the seizure was made in the premises of a legal entity, institution, or detachment, then a copy of the Protocol shall be delivered to its representative.

2.7 Real-time collection of traffic data

Article 20 of the Convention seeks to empower competent national authorities to collect, in real time, traffic data associated with specified communications within the territory of every Party, transmitted by means of a computer system. Proper implementation of Article 20 would require that the following is achieved:

1. Competent authorities are empowered to collect or record traffic data, through the application of technical means , in real-time, associated with specified communications within its territory, transmitted by means of a computer system;
2. Competent authorities are be empowered to compel a service provider, within its existing technical capability, to collect or record traffic data through the application of technical means, or to co-operate and assist the competent authorities in the collection or recording of traffic data;
3. Competent authorities are competent to ensure that service provider keeps confidential the fact of the execution of any of these powers, and any information relating to it.

2.7.1 Differentiation between real-time collection of traffic data and interception of content data

Armenian draft CPC regulates "Monitoring of Digital, including Telephone Communication" as one of the undercover investigative actions (Chapter 32). Draft CPC approaches this procedural power by regulating the object (paragraph 2) and methods (paragraph 3) of monitoring. Monitoring is defined (paragraph 1) as secret collection and storage of data envisaged by paragraph 2, using special and other technical means.

To begin with, it must be noted that pursuant to Article 256 of the CPC, monitoring cover both the contents of communication as well as information about communication. In the Convention's terms, this corresponds to notions of content and traffic data. Although different conditions and safeguards are applicable to monitoring of content and traffic data, differentiation between these measures is still not at appropriate level. For instance, paragraph 2 enumerates all data which are subject to this measure, without distinction between content information and other data. This distinction is introduced only in the next paragraph, where specific categories of data are associated with different methods of monitoring. But, paragraph 3 sub-paragraph 4 introduces additional power of "secret storage of the data envisaged by Paragraph 2 of this Article by natural persons or legal entities controlling it", which can, pursuant to paragraph 4, be applied in proceedings related to certain non-grave and medium-gravity crimes. Since paragraph 2 includes content data, literal reading of all these provisions might lead to the situation where no distinction between monitoring of content and traffic data exists. This would contradict both the purpose of paragraph 4 and would, at the same time, remove any distinction between interception of content and monitoring of traffic data. Such solution would not be in accordance with the text and the purpose of the Convention, nor would it satisfy the needs of law enforcement, which may require access to traffic data under less restrictive conditions than those used to access content data. Consequently, we propose that measures of collection of traffic data and interception of content data be completely separated, in different articles in the CPC.

2.7.2 Scope of traffic data monitoring

Turning to the scope of data which are subject to monitoring, and excluding content data, we see that "monitoring of digital, including telephone communication" measure covers the following information about communications. For the purpose of comparison, reference is made to the definition of "traffic data" in Art. 1(d) of the Convention.

Cybercrime Convention, Art. 1(d)	**Fixed telephone network, CPC 256(3)(1)**	**Mobile telephone network, CPC 256(3)(2)**	**Internet communication, CPC 256(3)(3)**
"traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.	b. Determination of the telephone number; c. Collecting and/or documenting the individual data of the subscriber of a particular telephone number, and the data necessary for determining the whereabouts and movement of the communicating parties at the starting time and during the telephone	b. Collecting and/or documenting the telephone communication starting date, beginning and end, telephone number, individual data of the subscriber of a particular telephone number, and the data necessary for determining the whereabouts and movement of the communicating parties	b. Collecting and/or documenting data through which it is possible to determine the geographic location, day, time, and duration of entering and exiting the Internet, including the Internet Protocol (IP) address, the name and user ID of the subscriber or Internet user, the telephone number through which he connects to the

	communication; d. In case of forwarding or transferring the telephone call—determination of the telephone number to which the call was forwarded;	at the starting time and during the telephone communication;	common telephone network, the Internet address, the name of the recipient of the Internet telephone call or any other data concerning facts, incidents, or circumstances related to such person in a form that allows or could allow identifying such person;

2.7.3 Conditions and safeguards

According to the current draft of the CPC, "Monitoring of Digital, including Telephone Communication" is one of the undercover investigative actions defined in Chapter 31. Conditions and safeguards applicable to this measure are stipulated below. Where necessary, relevant comments and recommendations are given.

Subsidiary application. Pursuant to Article 249(1), "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 at hand, and, at the same time, obtaining such Evidence in other ways is reasonably impossible". In the draft CPC, application of monitoring of communications to traffic data would require showing that obtaining evidence of significance to proceedings is "reasonably impossible". This is due to the fact that both interception of content and monitoring of traffic data are subject to same conditions and safeguards. If current "Monitoring of Digital, including Telephone Communication" measure is divided in two separate procedural powers, then it will become possible to apply different conditions and safeguards to each of them. In such circumstances, drafters of the CPC might consider lowering the requirements for accessing traffic data. For example, it could be stipulated that traffic data might be analysed if evidence cannot be obtained otherwise, or if that would be possible only under disproportionate difficulties.

Proper petition by the investigator. Pursuant to Articles 298 and 299 of the draft CPC, petition to perform undercover investigative action must be submitted to court by an investigator. Contents of such petition is stipulated in Article 299(1). When monitoring of digital communications is requested, petition must also contain "the respective telephone number, e-mail address, words or word combinations of interest for the search, or other relevant personal identification data" (Article 291(4) of the draft CPC). In general, we have no reservations regarding this provision. However, if specific power of monitoring traffic data would be introduced, then it might be useful to clarify that "other relevant personal identification data" might include IMSI number or IP address.

Judicial authorization. Pursuant to Article 249(2), undercover investigative actions should be based on a court decision. Petition to perform such action should be examined by the court immediately after it is presented by an investigator, and in any case not later than within three hours. Requirement that traffic data can only be monitored on the basis of court order is not inappropriate. But, if the national authorities consider that in certain cases court authorization would not be expedient enough, it might be advisable to introduce the possibility of urgent authorization by the prosecutor, with subsequent judicial supervision. However, this issue concerns general safeguards related to undercover investigative actions and is therefore not of primary concern in the context of Cybercrime Convention.

Inadmissibility of unlawfully obtained evidence. Pursuant to Article 250(1), information, materials, and documents obtained during the performance of an undercover investigative action, "obtaining which was not contemplated by the decision on performing such action, … may not be used as Evidence in the Criminal Proceedings and shall be subject to destruction, unless the Inquiry Body has acted in good faith". This provision is compatible with the Cybercrime Convention.

Scope of application in relation to criminal offences. According to current draft CPC, monitoring of traffic data would be possible in proceedings related to grave and particularly grave crimes, as well as certain non-grave and medium-gravity crimes (pursuant to Article 256(4)).

Pursuant to Article 14(3)(a) of the Convention, "each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21". However, it is also stipulated that "each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20".

In conclusion, we would urge the drafters of the CPC to reconsider the scope of traffic data monitoring and possibly broaden it. As a minimum, it should be ensured that monitoring of traffic data is possible in relation to relevant criminal offences established in accordance with Articles 2 through 11 of the Convention, as well as other relevant criminal offences committed by means of a computer system.

Scope of application in relation to persons. Pursuant to Article 250(2), monitoring of digital communications can be applied against (1) person concerning whom there are facts indicating the commission of the alleged crime, (2) accused or (3) "person concerning whom there is a justified assumption that he regularly directly communicated with or may reasonably communicate with an accused".

Enabling monitoring of traffic data of persons concerning whom there are facts indicating the commission of the alleged crime, and an accused is certainly proper. But, regarding "person concerning whom there is a justified assumption that he regularly directly communicated with or may reasonably communicate with an accused", the situation is less clear. The fact that certain person communicated or may reasonable communicate with an accused should not *per se* give rise to monitoring. Therefore, this provision should be revised and additional conditions necessary to authorize monitoring of third persons' communication should be introduced.

Protection of legally privileged communications. Pursuant to Article 250(7) of draft CPC, it is prohibited to apply monitoring of digital communications "if the person in respect of whom such action is to be performed communicates with his attorney or his designated confession priest. In any event, information obtained as a result of monitoring such communication shall be destroyed immediately".

This safeguard is relevant primarily in the context of interception of content. Where monitoring of traffic data is concerned, it should be made clear that attorney's and "designated confession priest's" communication should be exempted from monitoring, even if these persons would otherwise fall within the notion of "person concerning whom there is a justified assumption that he regularly directly communicated with or may reasonably communicate with an accused".

Formal requirements. Draft CPC imposes certain requirements regarding investigator's instruction to perform an undercover investigative action (Article 251) and the Protocol of such action (Article 252). These provisions are compatible with the Convention.

Recommendations:

In order to address some of the recommendations stipulated above (but not all of them), the following amendments can be introduced to Article 249 of the draft CPC:

"**Article 249. Monitoring of Digital, including Telephone Communication**

1. The monitoring of digital, including telephone communication is the secret collection and storage of the data envisaged by Paragraph 2 of this Article using special and other technical means by the natural persons or legal entities controlling them.

2. The following shall be subject to monitoring of digital, including telephone communication:

1) In case of fixed or mobile telephony—the telephone numbers of the communicating parties, the contents of the telephone conversation, the individual data of the telephone number subscriber, the starting date of the telephone communication, the starting and ending times, data necessary for determining the whereabouts and movement of the communicating parties at the starting time and during the telephone communication, the number to which the telephone call has been forwarded—in case of forwarding or transfer of telephone calls, and the contents of short text messages (SMS) and voice messages; and

2) In case of Internet communication, including Internet telephony communication and electronic messages transferred through the Internet - *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 (traffic data)*.

3. The following are the methods of monitoring digital, including telephone communication:

1) In case of the fixed telephone network:

a. Audio recording of the telephone communication or other methods of documenting its contents;

b. Determination of the telephone numbers that communicated with the telephone number in question;

c. Collecting and/or documenting the individual data of the subscriber of a particular telephone number, and the data necessary for determining the whereabouts and movement of the communicating parties at the starting time and during the telephone communication;

d. In case of forwarding or transferring the telephone call—determination of the telephone number to which the call was forwarded;

2) In case of the mobile telephone network:

a. Audio recording or otherwise documenting the contents of telephone communication, including short text messages (SMS) and voice messages;

b. Determination of the telephone numbers that communicated with the telephone number in question

c. Collecting and/or documenting the telephone communication starting date, beginning and end, telephone number, individual data of the subscriber of a particular telephone number, and the data necessary for determining the whereabouts and movement of the communicating parties at the starting time and during the telephone communication;

d. In case of forwarding or transferring the telephone call—determination of the telephone number to which the call was forwarded;

3) In case of Internet communication, including Internet telephone communication and electronic messages transferred through the Internet:

a. Audio recording of the communication or otherwise documenting its contents;

b. Collecting and/or documenting *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 (traffic data). Accessing and analysing information about communication (traffic data) can only be executed upon written and reasoned ruling issued by the judge, or if the person concerned gives his or her written consent.*

4) Secret storage of the data envisaged by Paragraph 2 of this Article by natural persons or legal entities controlling it.
4. The actions envisaged by sub-paragraphs 1(b), 1(d), 2(b), 3(b), and 4 of Paragraph 3 of this Article may also be performed in proceedings related to non-grave and medium-gravity crimes prescribed by Article 137, Article 144, Paragraph 2 of Article 158, Article 181, Articles 233-234, Articles 251 to 257, Article 263, Article 397.1 of the Criminal Code of the Republic of Armenia.
5. In case of the action envisaged by sub-paragraph 4 of Paragraph 3 of this Article, the stored data shall be immediately destroyed, unless they have been taken by the Inquiry body within 90 days of rendering the relevant Court decision.
6. When performing an undercover investigative action prescribed by this Article, telecommunications organizations shall be obliged, when demanded by the competent bodies, to provide technical systems and to create other conditions necessary for the performance of the undercover investigative action.
7. Managers and employees of communication services' providers shall be required to satisfy technical and other conditions necessary to enable accessing information about communication (traffic data) in real-time, in accordance with the law, and to take necessary measures to preserve confidentiality of conducting this measure. Communication service providers shall be required to keep records of all monitoring actions, and to make these records available to supervisory bodies."

2.8 Interception of content data

Article 21 of the Budapest Convention provides for what is considered the most intrusive of procedural powers, the interception of communications in real time. Interception powers are a tool of last resort for the investigation of serious crimes. These powers should be accompanied by strong safeguards and oversight. Interception as a covert power is a greater intrusion of privacy than any other form of electronic evidence, as it discloses private communications without the knowledge of the parties to that communication.

In the draft amendments to the Criminal Procedures Code (CPC), interception is addressed in the provisions relating to 'Monitoring of Digital, including Telephone communication'. The provisions, as drafted, do not differentiate between the access to the content of a communication and information about the communication (communications and traffic data). These powers need to be addressed separately and access to these powers should not be subject to the same authorisation. There are various arguments to support the separation of powers, including access to each power will have different investigative thresholds. Further, separate provisions will provide civil society with an understanding of the powers available to investigative agencies. Separating the investigative powers reduces the risk of a court reading down the provision and limiting the relevant authority's access to the content of a communication.

There is a general expectation that all people have a right to the privacy of their communications and a person seeking to lawfully access those communications must satisfy a court or relevant judicial authority that the intrusion to the privacy is commensurate to the investigation of the offence. It is important that these requirements relating to interception are separately stated in legislation and are of a higher standard to other powers including real-time access to traffic data.

The European Court of Human Rights, when considering covert surveillance, has noted it is preferable to have detailed law that clear and accessible. In addition, 'the Court places particular emphasis on the safeguards which must accompany surveillance and the keeping of records.'[1]

The interception of communications also requires, in most cases, the assistance of a service provider who is carrying the communication. The current draft of the CPC provides that 'when performing an undercover investigative action prescribed by the Article, telecommunications

[1] https://rm.coe.int/168067d214

organizations shall be obliged, when demanded by competent bodies, to provide technical systems and to create other conditions necessary for the performance of the undercover investigative action'[2]. Many international models for interception regulate how this assistance is to be provided, including using the relevant ETSI standards[3].

Recommendations:

A new provision should be drafted that provides for the interception of content in real time, separate from a provision to authorize access to real-time traffic data. Access to interception should always be authorised by a court or a relevant judicial authority, and the applicant should specify to the issuing authority the basis on which the interception should take place.

In addition, it is important that such request include the following data:

- name of the target if known;
- details of the service/s to be intercepted;
- nature of the offence/s being investigated;
- details of the alleged offence;
- any limitations or conditions upon the collection of the content;
- consideration of the privacy vs. the gravity of the offence; and
- proposed duration of the authority.

The legislation should provide details of the circumstances upon which a renewal of an authorization may be sought and specify the period of such a renewal. The legislation should also provide for the circumstances upon which an authorization may be revoked.

The draft CPC of Armenia should thus be amended to provide clear safeguards specific to the interception of communications. Safeguards are also necessary to protect the content once intercepted; this should include limitations on the handling and dissemination of the content both by the intercepting agency and the service provider. Any use of the content should be limited to the investigation of serious offences. Further access to the information for purposes other than the investigation of serious crime, should only be allowed in defined circumstances - for example, the investigation of a less serious crime where all activity is in an electronic form and no other techniques of investigation are available. There should also be destruction provisions for circumstances where content has been intercepted in error or is not relevant to the matter under investigation. Finally access to interception of content should be limited to situations where other investigative measure has been attempted but not successful.

Finally, consideration should be given to amending the draft CPC to include a level of reporting or oversight of these powers.

In order to address some (but not all) of the recommendations discussed above, a model provision to implement Article 21 of the Convention can be introduced to the draft Code of Criminal Procedure:

*"**Article 249[1]. Interception of content data in digital communications***

1. Interception of content data is an interference with private communications conducted without the knowledge of individuals concerned. Such interference can only be executed upon written and reasoned ruling issued by the judge.

[2] Article 256 (5) Monitoring of Digital, including Communication - Criminal Procedures Code

[3] http://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.03.01_60/ts_101331v010301p.pdf
http://www.etsi.org/deliver/etsi_es/201100_201199/201158/01.02.01_50/es_201158v010201m.pdf
http://www.etsi.org/deliver/etsi_ts/101600_101699/101671/03.14.01_60/ts_101671v031401p.pdf

2. Interception of content data can be ordered against the person for whom there is reasonable suspicion the he has committed, or has taken part in committing a serious or particularly serious crime under the Criminal Code of Armenia. This measure can also be ordered against the person for whom there is a reasonable suspicion that he delivers to, or receives from the perpetrator of such offences, information and messages in relation to these offences, or that the perpetrator uses their communication devices, or persons who hide the perpetrator or help him from being discovered.

3. In addition to information required for undercover investigative actions, judge's ruling authorizing interception of content data must refer to specific facts indicating existence of reasonable suspicion mentioned in paragraph 2 and reasoning justifying the necessity to apply this measure.

4. Interception of communication's content data is executed by responsible units of the bodies of internal affairs and bodies of security. These bodies are required to forward a copy of the judge's ruling to the communication service provider concerned. Destruction of intercepted content data, once the purposes for the measure have been achieved, should be monitored by independent, duly authorized authority.

5. Managers and employees of communication services' providers shall be required to facilitate surveillance and interception in accordance with the law, and to take necessary measures to preserve confidentiality of conducting this measure. Communication service providers shall be required to keep records of all interceptions, and to make these records available to supervisory bodies."

2.9 Optional recommendations on data retention (not directly related to the Budapest Convention on Cybercrime)[4]

Data retention is not addressed by the Budapest Convention, but generally data retention is a power that complements the powers articulated under the Convention. Unlike data preservation, data retention requires a service provider to retain information relevant to all communications for a set period of time. Data retention has been introduced in many jurisdictions. It had been introduced in the European Union by the Data Retention Directive of 2006, although the Directive was declared invalid by the Court of Justice of the EU (CJEU) in 2014. Nevertheless, many EU member States continue to operate data retention mechanism based on their national legislation.

In December 2016, the CJEU[5] found that EU law prevents its member States from "general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication" finding that it can only be done in certain circumstances and "solely for the purposes of fighting serious crime" such as protecting national security[6]. This decision infers that data retention should be a targeted approach not dissimilar to

[4] The Budapest Convention on Cybercrime does not foresee a general obligation to retain data but only the preservation of specified data within the context of a specific criminal investigation. General data retention obligations have been challenged by the European Court of Justice and courts in several member States of the Council of Europe. On the other hand, from a law enforcement perspective, many governments and criminal justice authorities consider data retention a necessary tool to ensure the availability of traffic data for criminal investigations.

[5] http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=631317

[6] ' Having regard to all of the foregoing, the answer to the first question referred in Case C-203/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the

data preservation under Article 16 of the Convention; at this stage, it is not entirely clear what the response of EU member States will be to this decision.

States beyond the EU jurisdictions regulate data retention irrespective of this debate; as an example, most recently, data retention was introduced into Australian law, requiring service providers to retain information for a period of up to 2 years.[7]

In considering the implementation of a data retention regime, it should be noted that any data retention regime is purely the mechanism to retain the data; it does not allow authorities to access the information without lawful means. Access to retained data should be for the investigation of serious crimes and the procedures used to access data should satisfy the Court or issuing authority that access to private information is proportionate to the crime being investigated.

Data retention should be implemented to assist in the investigation of serious crime. Data plays a central role in almost all serious criminal investigations, which is why it is so critical that agencies can lawfully access this kind of data about their investigations. For example, child exploitation investigations rely heavily on access to data, as perpetrators primarily share information online. Changing business models and technology means that many telecommunications companies are no longer retaining some types of data, or may not retain it long enough to be useful to law enforcement investigations.

Should the authorities of Armenia decide to pursue data retention the following may be considered:

- **Duration**: up to 1 year, consistent with most other international data retention models.
- **Destruction**: the regime should require destruction of the data once the information is no longer lawfully required.
- **Protection of data**: The retained data should be protected from unauthorised access or interference, with penalties considered for unlawful access.
- **Data to be retained**: the regime must be clear that the information to be retained does not include the content or substance of a communication. A clear data set must be developed and should include:
  - Subscriber information: information relating to a subscription to a service (e.g. name, address; this is not necessarily the data in electronic form);
  - Billing data: information relating to a subscriber's billing details and history;
  - Usage data: information relating to usage of a service (e.g. call records, telephone numbers of the parties involved in the communication, the date and time of a communication);
  - Equipment data: information relating to an end-user device or handset;
  - Network element data: information relating to a component in the underlying network infrastructure (e.g. location and identifier of a GSM base station - if this is not available from the usage data);
  - Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication;
  - Access to the information: Access to information retained under a data retention scheme should include clear provisions for access and use of information. This should include oversight and reporting;

---

general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication'

[7] https://www.ag.gov.au/dataretention

- In determining the information to be retained and the technical manner of which the information should be accessed, consideration may be given to the ETSI standards developed in response to the EU Data Retention Directive[8].

Recommendations:

Should the authorities of Armenia decide to pursue a data retention regime:

1. Provisions should be introduced into the telecommunications or electronic communications legislation to provide obligations for service providers to retain data for a specified period. The amendments should be consistent with the aim of conducting proceedings concerning alleged crimes, based on safeguarding human rights and freedoms.

2. A data set should be developed to define the information to be retained and include destruction provisions once the period of retention has expired. The data set should be consistent with the international standards already in existence.

3. The provisions should limit access to retained data for the investigation of serious offences and require lawful authority to access the information. The agencies who access the information should be subject to a level of accountability, whereby they must be satisfying a court or issuing authority of the need to access the information and satisfy the authority that the need to access the information is commensurate to the crime being investigated. It should be stipulated in law that retained data must be destroyed after retention period expires.

To guide the authorities in the development of relevant legislation, the following model provision may be used to introduce basic requirements of possible data retention legislation:

"Article ??. Data retention obligation

(1) Providers of electronic communications shall be obliged to retain electronic communications data, such as:

a. data necessary to trace and identify the source of a communication;
b. data necessary to identify the destination of a communication;
c. data necessary to identify the date, time and duration of a communication;
d. data necessary to identify the type of communication;
e. data necessary to identify users' communication equipment or what purports to be their equipment;
f. data necessary to identify the location of mobile communication equipment;
g. data relating to unsuccessful call attempts, whereby there is no obligation to retain data relating to unconnected calls;

- in order to make possible the conduct of the investigation, discovery and criminal prosecution of criminal offences, as well as protection of defence and national security, in accordance with special laws governing those activities. Competent authorities can gain access to these data in accordance with special legislation.

(2) Providers of electronic communications shall be obliged to retain data referred to in par. 1 in their original form or as data processed in the course of provision of communications networks and services. Providers shall not be obliged to retain data not originating from or processed by them.

(3) Providers of electronic communications must retain data referred to in par. 1 for the period of twelve months from the date of the communication.

[8] http://www.etsi.org/deliver/etsi_ts/102600_102699/102657/01.14.01_60/ts_102657v011401p.pdf See specifically Annexure H.

(4) Providers of electronic communications shall comply with the data retention obligation in the manner that retained data, together with all other necessary and related data, may be delivered without delay to the competent body referred to in paragraph 1 of this Article.
(5) Providers of electronic communications must in particular apply the following data security principles with respect to retained data:

a. *the retained data shall be of the same quality and be subject to the same security and protection as those data on the provider's electronic communications network;*
b. *the retained data must be protected in the appropriate manner against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;*
c. *access to retained data must be exclusively limited to authorised persons of competent bodies referred to in paragraph 1 of this article;*
d. *the retained data must be destroyed after the expiry of the period of retention referred to in paragraph 3 of this Article.*

(6) For the purpose of application of data security principles referred to in paragraph 5 of this Article, the providers of electronic communications must ensure at their own expense the implementation of all appropriate technical and organisational measures.
(7) The provider of electronic communications must appoint a person responsible for the enforcement of measures and standards of information security.
(8) Providers of electronic communications must keep a list of end-users of their services which they are obliged to deliver to the competent authorities referred to in paragraph 1 of this Article upon their request. The list of end-users must contain all the necessary data enabling unambiguous and immediate identification of every end-user.
(9) Providers of electronic communications must establish procedures with a view to fulfilling the obligations referred to in this Article and deliver to the competent authority, upon its request, information on the organised procedures.
(10) Providers of electronic communications must keep information about the number of received requests to access data, the legal basis for the submission of requests and the type of data delivered upon the received requests. This data must be made available to supervisory authorities, upon their request."

3 Conclusions

The recommendations and proposals made by Council of Europe are submitted for consideration by the authorities of Armenia.

The proposals of sections 2.1 to 2.8 are aimed at ensuring compliance with the procedural law provisions of the Budapest Convention on Cybercrime. This in turn should facilitate domestic investigations on cybercrime and other offences involving electronic evidence, strengthen the legal basis for law enforcement requests for data to service providers and allow for more effective international cooperation while respecting rule of law requirements.

The proposals of section 2.9 are made in case the authorities of Armenia decide to maintain a general obligation to retain traffic data. They are designed to enhance legal certainty, proportionality and foreseeability.

The Council of Europe remains available to provide further assistance to ensure completion of these reforms.