Cybercrime@EAP III

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

2016/DGI/JP/3608
30 June 2017

Suggestions for draft amendments to procedural legislation of Azerbaijan and other recommendaitons 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 Zahid Jamil, Marjan Stoilkovski and Markko Künnapu 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. During Cybercrime@EAP I, Eastern Partnership countries concluded that international and public/private cooperation, in particular with regard to access to electronic evidence for criminal justice purposes, were among strategic priorities for the region. 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. As 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), the importance of proper legislative background for public-private cooperation on cybercrime and electronic evidence was repeatedly highlighted, also in terms of compliance with the Convention.

The project country team of Azerbaijan has indicated, throughout Regional meetings and in-country events of the project (in particular, "Workshop on public-private cooperation between the law enforcement and ISPs" on 12-14 October 2016, and "Workshop on reform of legislation to ensure compliance with Articles 16 and 17 Budapest Convention on Cybercrime" on 13-15 February 2017 under the Cybercrime@EAP II project) that the Azerbaijani authorities are willing to remedy outstanding issues of compliance of their national 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 Azerbaijan 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, Mr Marjan Stoilkovski from Former Yugoslav republic of Macedonia, Mr Markko Künnapu from Estonia and Mr Zahid Jamil from Pakistan, to provide a review of the existing provisions of laws in Azerbaijan in terms of compliance with the Council of Europe Convention on Cybercrime and other applicable standards. The discussion with Azerbaijani counterparts on 10-12 May 2017 in Baku, organized under the Cybercrime@EAP III project, allowed experts to discuss the details of the existing provisions and suggest some recommendations for improvement, which are outlined below.

For ease of reference and clarity, the proposed amendments are in *italics*.

2 Recommendations proposed by the experts

2.1 Definition of electronic evidence

The Code of Criminal Procedure of Azerbaijan does not explicitly recognize electronic evidence as part of material evidence. Material evidence is defined under Article 128.1 of the Code, which provides that material evidence must be an "item". This provision thus suggests that the term "material evidence" only encompasses materials that are in physical form.

The term "documents", defined under Article 135 of the Code, includes "paper, electronic and other materials". Article 135.2 of the Code provides documents which have "the characteristics described in Article 128.1 of the Code may also be considered as material evidence". However, given the ambiguity regarding the inclusion of electronic evidence within the definition of material evidence, it is unclear whether electronic documents have the characteristics described in Article 128.1 of the Code.

The context in which the term "material evidence" has been used in the Code also suggests that the term was not intended to apply to electronic evidence. For instance, Article 129, which describes the manner in which material evidence is to be preserved, provides that material evidence "be packed and kept in sealed form in the case file". While this may be appropriate for physical evidence, it may not necessarily apply to intangible electronic evidence (i.e. in the form of stored computer data).

The lack of or ambiguity regarding the inclusion of electronic evidence within the definition of material evidence poses a problem with respect to applicability of procedural powers - including the power to order preservation, production and seizure - to evidence in electronic form. Thus it is recommended that the concept of electronic evidence be included as part of material evidence under Article 128 of the Code. An amendment which specifically recognizes materials in electronic form as part of material evidence would assist in this regard.

Recommendation:

Amend Article 128.1 of the Code:

"128.1. *Any material, whether in physical or electronic form,* or any item that can help to determine circumstances of importance to the prosecution because of its characteristics, features, origin, place and time of discovery or the imprints it bears may be considered to be material evidence."

2.2 Admissibility and chain of custody

There are no specific rules regarding admissibility and chain of custody of electronic evidence, and the general rules of admissibility and chain of custody in the Code of Criminal Procedure apply to both physical evidence and electronic evidence.

Article 129 of the Code provides for the preservation of material evidence and other items. It requires that all material evidence, where possible, is to be "packed and kept in sealed form in the case file". It further provides that if the material evidence is "of a large size, it shall be given for safekeeping to an organisation, institution or appropriate person".

The powers conferred under Article 129 of the Code are thus appropriate for physical evidence, which may be sealed and be physically kept with the case file. However, given that electronic evidence may be in the form of computer data stored in a computer system or an immovable computer data storage medium, it may not be possible for the computer system or computer data storage medium to be physically seized and kept with the case file.

Moreover, in case of electronic evidence, it may not be sufficient for the purposes of maintaining chain of custody and integrity of electronic evidence to merely keep such evidence in the case file. Additional measures may have to be mandated to ensure that the integrity of the data is maintained and secured.

Given the unique characteristics of electronic evidence, provisions designed to ensure admissibility of physical evidence may not be effective in ensuring the integrity and chain of custody of electronic evidence. Thus it is recommended that Article 129.1 be amended to distinguish the requirements for preservation of electronic and physical material evidence.

Recommendation:

Amend Article 129.1 of the Code:

"129.1. Material evidence, *if in physical form,* shall where possible be packed and kept in sealed form in the case file; if it is of a large size, it shall be given for safekeeping to an organisation, institution or appropriate person, subject to their consent. *Material evidence, if in electronic form, shall be preserved in a manner so as to secure and maintain its integrity*."

2.3 Definitions of categories of data

The Code of Criminal Procedure does not provide for any specific definitions of any kind of data. The power of interception of communications, for instance, applies generally to "conversations held by telephone and other devices and of information sent by communication media and other technical means". Other than this category of data, there is no recognition of subscriber information or traffic data in the Code. Procedural powers are generally applicable; and there is ambiguity as to whether they extend to any type of computer data, let alone specific types of computer data.

The Budapest Convention recognizes three categories of information/data that are relevant for the purposes of procedural powers relating to the collection of electronic evidence. These categories are: subscriber information, traffic data and content data. Each type of data/information has, at some instances, different procedural powers associated with it, and each may come with varying levels of safeguards and guarantees, including separate grounds, thresholds and mechanisms applicable to each category.

Given that the Code does not recognize different types of data, the procedural powers within the Code, when exercised with respect to such data, may result in it being either too easy to obtain highly privacy-intrusive data (i.e. content data), or too difficult to obtain less privacy-intrusive data (i.e. traffic data).

It is thus necessary that some necessary definitions of term that are consistent with the Budapest Convention are part of the Code, and it is also recommended that the Code provides for some of the more specialized definitions (i.e. subscriber information) as a part of procedural powers corresponding to such type of data.

Recommendation:

Amend Article 7 of the Code to include the following definitions:

"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"service provider" means:
1. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
2. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

"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.

2.4 Expedited preservation and provisional disclosure of stored computer data

There is no provision in the Code relating to expedited preservation of stored computer data and partial disclosure of preserved traffic data. Article 129 of the Code provides for the preservation of material evidence and other items. Given that the term "material evidence" appears not to include stored computer data or traffic data, Article 129 of the Code does not provide procedural powers equivalent to Articles 16 and 17 Budapest Convention.

Article 16 Budapest Convention provides for the expedited preservation of stored computer data. In particular, it enables the competent authorities to order expedited preservation of stored computer data (including traffic data) where there are grounds to believe that the computer data is vulnerable to loss or modification. Article 129 of the Code does not provide the same power, and given its generality, it would not fully encompass Article 16 Budapest Convention.

Moreover, Article 129 of the Code does not enable the exercising of procedural powers to seek partial disclosure of preserved traffic data as provided under Article 17 of the Budapest Convention. This procedural power includes the ability to order immediate disclosure of sufficient amount of traffic data to enable the identification of service providers involved in the chain of transmission of a communication, as well as the path through which a communication has been transmitted.

Thus given that Article 129 of the Code is not appropriate for electronic evidence and it is missing integral elements of Articles 16 and 17 Budapest Convention, a possible remedy is to insert a new provision that provides specifically for the expedited preservation of stored computer data and partial disclosure of preserved traffic data.

Recommendation:

Add the following provision to the Code:

*"**Article 142[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 or prosecutor can issue an order obliging any natural or legal person in whose possession or under whose control such data is believed to be located, or any person 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. Data preservation order 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.
3. Data preservation order, where necessary, shall oblige a person 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

Article 143 of the Code provides for the collection of evidence during investigation and court proceedings. Given that the Code does not distinguish between electronic evidence and physical evidence, this Article 143 of the Code applies generally to all types of evidence, and is not specific to electronic evidence.

With respect to the power to seek production, Article 143 of the Code authorizes the competent authorities to request the presentation of "documents". The term "document" has been defined in Article 135 of the Code as follows: "Paper, electronic and other materials bearing information which may be of importance to the prosecution, in the form of letters, numbers, graphics or other signs, shall be considered as documents." Thus, to the extent of requesting presentation of electronic documents, it appears that Article 143 of the Code is the means for realizing the procedural power under Article 18 Budapest Convention.

However, Article 143 of the Code does not distinguish between requesting handover of stored computer data and subscriber information. Thus, it also does not specifically provide for the ordering of subscriber information in the possession or control of service providers offering services within the territory of Azerbaijan, regardless of whether the service providers are located in Azerbaijan.

Moreover, the use of the term "request" suggests that the measure of seeking presentation of a document may not be a compulsory measure. If so interpreted, Article 143 of the Code may be inconsistent with Article 18 Budapest Convention, which requires that Parties should compel persons in possession or control of computer data (and service providers in possession or control of subscriber information) to produce such data upon being served with a production order by the competent authority.

Article 143 of the Code does not provide for any procedural safeguards with respect to the exercise of the power of request for information. Article 143.2 of the Code suggests that the preliminary investigator, investigator, prosecutor or court each have the power to request presentation of documents. Thus, the preliminary investigator, investigator or prosecutor is not required to seek prior permission from an independent officer, and there is no requirement for any independent supervision with respect to the exercise of this power. To this extent, it appears that Article 143.2 of the Code may be inconsistent with the requirements of Article 15 Budapest Convention.

Recommendation:

Amend Article 143.2 of the Code:

143.2. During the process of collecting evidence, the preliminary investigator, investigator, prosecutor or court shall have the right, at the request of parties to the criminal proceedings or on their own initiative, to request the presentation of documents and other items of significance to the prosecution by individuals, legal entities, officials and the authorities which carry out search operations, and to request checks and inspections by the authorized authorities and officials. *During the process of criminal proceedings, the court shall have the right, at the request of the parties of the criminal proceedings, to order:*

143.2.1. a person 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;

143.2.2. a service provider offering its services in the territory of Azerbaijan to submit subscriber information relating to such services in that service provider's possession or control.

143.2.3. For the purposes of this Article, subscriber information means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

- *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, billing and payment information, available on the basis of the service agreement or arrangement;*
- *any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.*

2.6 Search and Seizure

Computer data are specific by its nature, and we need to implement specific mechanisms for efficient seizing of computer data. Computer data or electronic evidence is highly volatile, that is challenge for criminal justice authorities. Having appropriate legal ground for search and seizing of computer data is more than needed for criminal justice authorities not only for cyber crime cases but also for any other criminal case. The computer data in many cases are not needed to the criminal justice authorities only for a purpose of evidence, but also for the purpose of data and information that will be use to support the investigation.

Article 19 of the Cybercrime Convention requires that every Party adopts legislative and other measures necessary to empower the competent authorities to achieve full purpose of Article 19, to ensure that criminal justice authorities can:

- conduct measure of search of similar accessing,
- expeditiously extend such measure to linked systems,
- seize computer system, mediums or data,
- order any person who has knowledge or information necessary to conduct search to provide them.

Criminal justice authorities must be able to search or similarly access computer system, parts of computer systems, storage mediums and computer data.

Criminal justice authorities must have the power to expeditiously extend previously mentioned power to other computer system or its part if, while conducting a search of the initial system, they develop grounds to believe that the data sought is stored in that other system, and data in question is lawfully accessible from or available to the initial system.

Criminal justice authorities must be empowered to order anyone who has knowledge or information about functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information to conduct a search.

Criminal justice authorities must be empowered to seize or similarly secure computer data, which includes powers to:

- seize (take away) or similarly secure computer system, parts of it or storage mediums,
- make and retain a copy of computer data;
- maintain the integrity of the relevant stored computer data;
- render inaccessible or remove those computer data in the accessed computer system.

In this light, the existing Article 242 from the Code of Criminal Procedure provides for legal basis for conducting a computer search, but needs specific provision that will cover search and seizing of computer data. The law should allow for legal grounds for the criminal justice authorities to search computer systems and seize computer equipment, as well as seize computer data.

The proposed amendments will give power to the criminal justice authorities (investigation authority) in the country to access in the computer and search into computer system on the scene, but also to access computer systems on another place on the territory of Azerbaijan. The

added provisions in the Article 242.4 also give power to the investigative authority to search the computer data in the computer system and seize particular computer data.

It is very important the proposed provisions to guaranty the integrity of the computer data in the computer, computer systems and seized computer data. In addition, the proposed provision gives legal base for involving experts to assist the authorities in the process of search and seizing computer equipment and computer data, because not always criminal justice authorities have appropriate knowledge of the computer systems and platforms in order to efficient perform the search and seizing and guaranty the integrity of the computer systems and computer data.

Recommendation:

The following changes in the Chapter XXX of the Code of Criminal Procedure are necessary:

"**Article 242. Conduct of a search**

242.1. 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, the investigator may conduct a search.
242.2. A search may be conducted with the aim of finding persons or animals being sought or human or animal remains.
242.3. Objects and documents which may be of significance as evidence may be impounded by the investigator once it has been established on the basis of the evidence collected or the material discovered in a search operation where or in whose possession they are.
242.4. For the purposes of this Chapter, during any search conducted of a premises or a person and any seizure of any object, document or item or computer system, computer data or computer storage media, the investigator or specialist conducting the search or seizure may:
242.4.1. search or similarly access computer system or part of it and computer data stored therein and/or a computer-data storage medium in which computer data may be stored,
242.4.2.i. where there are grounds to believe that the data sought is stored in another computer system or part of it in territory of Azerbaijan, and such data is lawfully accessible from or available to the initial system, the investigator or specialist shall be able to expeditiously extend the search or similar accessing to the other system within the territory of Azerbaijan;
242.4.2.ii. where there are grounds to believe that data sought is stored in another computer system or part of it in an unknown territory or a territory outside Azerbaijan, and such data is accessible from or available to the initial system, the investigator or specialist shall be able to expeditiously extend the search or similar accessing to the other system regardless of whether the computer system or computer data is outside the territory of Azerbaijan or its location is unknown, and in all a such cases the Court shall be informed of such extended search or seizure to seek approval of the court;
242.4.3. seize or similarly secure a computer system or part of it or a computer-data storage medium;
242.4.4. make and retain a copy of those computer data;
242.4.5. maintain the integrity of the relevant stored computer data;
242.4.6. render inaccessible or remove those computer data in the accessed computer system;
242.4.7. order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in this paragraph.

Article 243. Grounds for conducting a search and seizure

243.2. The decision to authorise the search or seizure shall state the following:
…

243.2.6. in the case of a decision authorising seizure, the objects and documents to be impounded, *including computer data. In case of computer data, the decision should enable an identical reproduction of the original computer data in a manner so as to secure and maintain its integrity, unless there are compelling reasons to impound the physical devices (computer system or computer storage medium) containing the computer data for the interest of administration of justice.*

243.3. In circumstances which admit no delay, the investigator may conduct a search or seizure without court permission only if there is precise information indicating that:
243.3.1. objects or documents, items or *computer data stored in any computer system or a computer-data storage medium* concealed in a residential building constitute proof of the commission of an offence or of preparations for the commission of an offence against a person or the state;

Article 245. Rules governing searches and seizures

245.1. An investigator shall be entitled to enter a residential or other building and *access or seize computer system by technical means* as stipulated in Article 243.2.6 found within such building on the basis of the court decision concerning the search or seizure.
…
245.8. During a search or seizure, all objects, items and documents shall be presented to the participants in the investigative procedure and their quantity, size, weight, material and other special features shall be specified as part of a detailed description. The objects, items and documents shall be packed and, if necessary, sealed by the investigator. *Material evidence in electronic form shall be preserved in a manner so as to secure and maintain its integrity*."

2.7 Real-time collection of traffic data and interception of content data

Article 259 of the Code of Criminal Procedure provides for the interception of communications. It also implements Articles 20 and 21 Budapest Convention that provide for two procedural powers: real-time collection of traffic data and real-time interception of content data.

The purpose of the proposed amendments (found below) is to fill certain gaps in the legislation related to real-time collection of traffic data and interception of content data as well as bring the legislation in line with Articles 20 and 21 Budapest Convention.

Although the Code had already in place provisions enabling interception of phone and other communications, certain amendments in order to increase legal clarity and foreseeability are needed. As these measures directly restrict the rights to the protection of private life and personal data, conditions and safeguards need to be built in as well.

The newly proposed paragraph 1^1 of Article 259 provides for the detailed description on how interception of communication transmitted by the computer system takes place as well as conditions and safeguards. Due to the invasive nature of the measure, the new paragraph 1^2 of the same Article suggests that measure could be limited to the serious and particularly serious crime.

As interception of communication often requires active cooperation by the service provider side, certain obligations for them must be foreseen. In order to ensure the interception by technical means, service providers must co-operate and assist law enforcement authorities while performing their duties.

Recommendations:

Add the following text to Article 259 of the Code:

"**Article 259. Interception of conversations held by telephone and other devices, of information sent by communication media and other technical means, and of other information**

...

259.1[1]. Interception of communications sent by communication media and other technical means may be performed by collecting or recording, through the application of technical means, of the traffic data, in real-time, associated with specified communications in the territory of Azerbaijan transmitted by means of a computer system. On the basis of a reasoned request by the investigator and appropriate submissions by the prosecutor in charge of the procedural aspects of the investigation, the court may order a service provider operating on the territory of Azerbaijan and within its existing technical capability, to collect or record through the application of technical means or co-operate and assist the competent authorities in the collection or recording of traffic data in real-time, associated with specified communications in the territory of Azerbaijan transmitted by means of a computer system.

259.1[2]. The court may, by its decision, only in cases of serious and particularly serious crimes as defined by the Criminal Code of Azerbaijan, authorize interception of the content of communications sent by communication media and other technical means to be performed by authorized authorities in order to:

- collect or record through the application of technical means on the territory of that Party, and

- compel a service provider, within its existing technical capability:

i) to collect or record through the application of technical means on the territory of that Party, or

ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2.8 Optional recommendation on data retention (not directly related to the Budapest Convention on Cybercrime)[1]

Mandatory preservation or retention of telecommunications data has been quite a controversial issue since it was widely introduced in different European Union Member States. Although it was used in several European countries earlier, it became a standard at European Union level in 2006, when so-called Data Retention Directive was adopted in 2006.[2] According to the Directive, Member States had to enact legislation at national level that would oblige telecommunication service providers to keep certain categories of data for a determined period of time. Categories of data included subscriber information and traffic data for both telephone and Internet service[3]. The time for the retention of data was from 6 months to 2 years. When the Directive was implemented, the period of 1 year became the average retention period. Although the Directive provided the data

[1] 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.

[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0024

[3] See Article 5 of the Directive.

retention for the detection and investigation of serious crime, many Member States went beyond and enabled the use of data also for other criminal offences.

However from the beginning the Directive and its implementation in several Member States was challenged, because different human rights, privacy and data protection organisations argued that the data retention framework violated fundamental rights and personal data protection rules.

European Court of Justice has so far given two judgments on the matter. In April 2014 the Court came to the conclusion that the Directive was not in line with the European Charter of Fundamental Rights and declared the Directive invalid.[4] Although the Directive was declared invalid, the judgment didn't affect national legislation of the Member States. Still in several Member States cases were brought to their Constitutional courts and in many cases national legislation on data retention was declared invalid as well. In the latest judgment of the Court in December 2016 the court decided that national legislation implementing the Directive was also in conflict with Charter of Fundamental Rights and data protection rules.[5]

At the moment Member States are analysing the impact of the judgment and try to find ways to accommodate the concerns of the court and to improve national legislation. A working group on data retention issues was established and discussions are being held. Several Member States have urged the European Commission to come out with a new proposal for a Directive that would meet the needs and criteria of the judgment.

Currently there are several Member States that do not have data retention framework in place. Lack of data, however, is affecting not only these particular countries, but also countries that would like to send whether preservation requests or production orders to them. As without data retention framework telecommunications data is deleted, it cannot be kept or accessed at a later stage. That has lead to a situation where mutual assistance requests are denied, because data is no more available.

From the practitioner's point of view, data retention framework was and still is a useful and important tool to fight crime. Using retained telecommunication data enables not only to investigate cybercrime, but whatever crime related to the use of communications by phone or the Internet. It is not a substitute or alternative to the preservation of data, because it has different nature. Preservation is possible for data that exists. Data retention framework in turn enabled law enforcement authorities literally go back in time and ask access to so-called historic data related to communications that had taken place some time ago.

Although the Budapest Convention does not regulate the retention of data, it has still stressed for several times in the Cybercrime Convention Committee that tools like preservation of data and data retention complement each other. To ensure effective investigations, State Parties should preferably implement both.

Recommendation:

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

[4] 2014 ECJ Judgment C-293/12 Digital Rights Ireland
http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=705067

[5] 2016 ECJ Judgment C-203/15 Tele2 Sverige
http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=705236

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 that 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.

(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."

2.9 Optional recommendations on interagency and public-private cooperation on cybercrime and electronic evidence

There are several entities on the national level that have significant role in fighting and preventing cybercrime. According to the legislation and the mission, each of them should work in their own areas but in any case to be prepared to react in cooperation with the other institutions. The cooperation among the institutions can be impossible or complicated if there is no appropriate law in place, procedures and system which will define the exact role of the relevant institutions. Such system will facilitate the cooperation but also will draw the directions for the institutions for developing and building own capacities in order to meet the potential requirements in the situation of cybercrime and need of investigation.

The basic principle of information exchange and cooperation is to keep it as simple as possible. A hierarchical information sharing system usually does not work in the practice. Having one common accepted system by all institutions/actors is one of the best options, which at the same time is very simple for implementation. This approach allows them to easily follow all the processes and changes. Most of the information will be shared according to the system and its procedures. The best solution for this approach is if one of the involved institutions takes the responsibility of managing all the information as well as information sharing. Taking into account the position of the all the institutions connected with the area of cyber security, the national CSIRT/CERT can be considered as entity for taking this responsibility.

Public-private cooperation on cybercrime and electronic evidence is another matter of cooperation that primarily seeks to enhance access by the law enforcement to the data held by the Internet service providers. However, cooperation with the Internet service providers does not mean only cooperation with the Internet (access) service providers, but also cooperation with the any entity/company that offers any service on Internet and holds some type of data, or, in other words, cooperation with the private sector. Some providers hold only subscriber data (IP address), but some providers could hold traffic and content data that can be accessed by criminal justice authorities.

Likewise, public-private cooperation does not only imply sending the request for disclosure of data held by the service providers or entities that offer some service on the Internet. Usually the

criminal justice authorities need more support from the relevant authorities or entities that offer some service on Internet to be able to receive reliable data in the shortest time possible.

The challenge in reporting the cybercrime cases and computer incidents is more common for the private sector and is one of the challenges for public-private cooperation. Private entities are sometimes not aware that their organizations had experienced one or more cyber security incidents, and therefore indicate that they had not experienced any such incidents when asked. In addition, victimized organizations may be reluctant to report breaches due to a range of reasons, such as:

- believing the incident was not serious enough to warrant reporting it to law enforcement and other competent agencies,
- believing that there is little chance of a successful prosecution (they are not aware of the capacities of criminal justice authorities),
- fearing negative publicity and that reporting would result in a competitive disadvantage.

Recommendation:

The authorities of Azerbaijan can be guided by the following principles in this regard:

1. Developing procedures for cooperation between criminal justice authorities and the national CSIRT/CERT.

These procedures should give a framework of cooperation and also to define the responsibility of the criminal justice authorities and the national CSIRT/CERT. The procedures need to define the type of data than will be exchanged and the model that will be used for exchanging the data. Additionally, those procedures should confirm the existing cooperation and mutual support and to cover the planned improvements of mutual support and sharing the capacities, in the following ways:

1.a. Defining the responsibility for cybercrime and cyber incident situations.

Very often the entities that have responsibility in the same areas also have issues in the situation when need to act on the same case. It's more than needed to generally divide the responsibility on each entity in particular cases.

1.b. Developing system for capacity building in area of handling of cybercrime incidents and handling electronic evidence.

The responsibility for investigating and preventing cybercrime is not only the domain of criminal justice authorities, but for all relevant entities and individuals in the country. It needs model for sharing capacities and capability and joint approach to building capacities.

1.c. Agreement and protocol for exchanging of information for cyber crime trends/treats and good practices.

Criminal justice authorities are receiving information from different sources (international police organizations) on current trends and threats in area of cybercrime and cyber security. From other side, private sector has other sources of information about the same. The agreement/protocol for exchanging those types of data will improve the response to cybercrime and cybersecurity challenges from criminal justice authorities, private sector and CSIRT community.

2. Developing procedures for legally binding requests which includes appropriate due diligence measures, for the issuing and processing of legally binding requests, and ensure that requests are carried out pursuant to the agreed procedures.

Procedures that will define the form, mode and channel for sending request for data to the national Internet service providers including emergency requests.

3. Organizing practical exercises for cybercrime and cyber incidents in order to better understand the responsibility and capability of each entity and also to identify the potential gaps in procedures and capacities.
The practical exercise for cybercrime and cyber incidents will improve the coordination and improve the efficiency of all entities involved in the real-case scenarios. This can be good opportunity to identify real capacity and capability of each entity and, based on that, plan future activities for capacity building.

4. Developing efficient cyber crime reporting system/procedures that allow private sector to report more computer incidents and criminal justice authorities to ensure confidentiality of data received.
The reporting functionality is service that gives opportunities to all companies and institutions to report any cybercrime cases or cyber security issues. This procedure allows submitting report for the criminal case and submitting the relevant data that are held by the reporting entity. This functionality could be available for the criminal justice authorities and for the entities that are reporting the particular issue. Some of the reported cases will be handled by the CSIRTs and according to the case, will be filed to the cybercrime unit or will be considered only as a subject of examination and analysis. In some specific cases, when the cyber attacks are directed against the critical infrastructure, or the attacks are against the national security and defence, other institutions can also be involved.

5. Designate personnel and contact points - interaction between criminal justice authorities and service providers should be limited to trained personnel; defining the responsibilities of the contact points.
Establishing a list of adequate experts from any entities involved in the cybercrime issues will improve communication, coordination and the joint response to cybercrime.

6. Organization of and participation in meetings between criminal justice authorities and private sector (Internet service providers) in order to exchange the practical experience and identify the issues for improving cooperation and exchange of information.
This implies planning and holding regular meetings for exchanging experience and ideas for improving cooperation and improving capacities, and with that improving also the efficiency of the response to cybercrime challenges by the criminal justice authority.

3 Conclusions

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

The proposals of sections 2.1 to 2.7 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 sections 2.8 and 2.9 are made in case the authorities of Azerbaijan 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.