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 Ukraine 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 Marko Juric, Nigel Jones 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

On 1 July 2006, Ukraine became a Party to the Budapest Convention on Cybercrime. This treaty requires Parties to provide in their domestic laws not only for the criminalisation of offences against and by means of computers but also for procedural law powers to enable competent criminal justice authorities to secure electronic evidence in relation to any crime. Such powers are necessary for domestic investigations but also a pre-condition for effective internatinal cooperation. They are furthermore a condition for obtaining data, and thus evidence, from private sector entities such as service providers.

Although Ukraine has been a Party to the Budapest Convention for more than ten years, domestic procedural law is not yet in line with the obligations under this treaty.[1] This hinders domestic investigations, public/private cooperation and international cooperation.

Further to a specific request by the authorities of Ukraine during the launching conference of the Cybercrime@EAP III project (Kyiv, April 2016), it was agreed to address the strengthening of criminal procedure law as a matter of priority under this project.

In September 2016, Council of Europe experts presented a study on current and proposed practices and solutions to ensure compliance with the procedural law provisions of the Budapest Convention. In parallel, a working group identified and assessed problems in the legislation of Ukraine representing major obstacles to public-private cooperation regarding cybercrime and electronic evidence. This resulted in an initial report.

On 14 September 2016, the Council of Europe furthermore received a letter from Mr. Oleksandr Danchenko, Chair of Parliamentary Committee on Informatisation and Communication of Ukraine, requesting the expertise of the Council of Europe on draft laws related to telecommunication and information technologies. As the draft laws also concerned the matter of public-private cooperation on cybercrime and electronic evidence, the same group of experts was asked to integrate findings in this respect in their assessment report.

At the time, the following conclusions and recommendations were provided by the experts:

- Organization and ownership of legal reform on the issue needs to be made clear for effective management of the process;
- Provide clear separation of investigative authority between the security and law enforcement when it comes to cybercrime and electronic evidence;
- Continuous training and specialization of criminal justice personnel is necessary;
- Clear definitions of electronic evidence, as well as definitions of subscriber information, traffic data and content data would increase predictability and foreseeability of law;
- Introduce specific powers for the preservation of data pursuant to Articles 16 and 17 of the Cybercrime Convention and enable sending and receiving preservation orders and similar requests electronically;
- Introduce clear and explicit obligation for the service providers to retain data about electronic communications, provide clear rules for accessing and use of retained data, create appropriate and independent supervision and stipulate in law that retained data must be destroyed after retention period expires;

[1] See among other things, the assessment of preservation provisions by the Cybercrime Convention Committee (T-CY) which has found Ukraine not be in line with the Convention and requested "the authorities of Ukraine to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime, including through specific preservation provisions".

- Introduce production order provisions pursuant to Article 18 of the Convention as an alternative to powers of search and seizure;
- Review the rules on search and seizure in order to cover the collection of electronic evidence, including the possibility of copying necessary data, extended search possibilities with regard to lawfully accessible data, and extended blocking/freezing possibilities under Art. 19 of the Cybercrime Convention;
- Review the limitations and safeguards for the application of monitoring and interception provisions pursuant Art. 20 and 21 of the Convention, especially with regard to detailed requirements developed in the case-law of the European Court of Human Rights;
- Ensure compatibility of measures provided by the Law on Operative and Investigative Activity with evidentiary requirements of the Criminal Procedure Code, including the conditions and safeguards contained therein;
- Blocking and take-down of the illegal content on the Internet should be regulated on the basis of proportionality requirements;
- Consider drafting specific rules on collection of electronic data applicable in urgent cases;
- Consider concluding Memoranda of Understanding or similar cooperation agreements between the law enforcement authorities and service providers.

Based on these recommendations, and following a series of working meetings with Ukrainian counterparts in February and April 2017 within the framework of the CyberCrime@EAP III project, three Council of Europe experts[2] developed the **draft amendments** below meant to ensure closer compliance of Ukraine with the corresponding provisions of the Budapest Convention on Cybercrime.

[2] Nigel Jones (United Kingdom), Markko Künnapu (Estonia) and Marko Juric (Croatia).

2 Text of amendments as proposed by experts

2.1 Investigative jurisdiction to investigate cybercrime offences

Article 216. (Investigative jurisdiction) should be amended by inserting a new paragraph 2[1] as follows:

2[1]. Investigators of bodies of security shall conduct pre-trial investigation of crimes specified in Chapter XVI of the Criminal Code of Ukraine, if crimes pose a threat to the vital interests of Ukraine. Disputes concerning jurisdiction will be settled by the chief of a higher-level prosecutor's office.

Explanatory note:

Currently it is not very clear how powers and competences regarding the investigation of cybercrime offences are divided berween different authorities. The law should provide for clear rules on investigative powers and competences of both Security Service and police. As the law already provides for provisions enabling the conduct of pre-trial investigations by the bodies of security when it comes to serious crimes against the state, similar logic and provision could cover also cybercrime. offences. Clear provision would decrease the jurisdiction conflicts between the investigation authorities and would give explicit powers to the prosecutor office to decide which authority would be the most appropriate to investigate particular case.

2.2 Definition of electronic evidence

1) Article 84 (Evidence) should be amended as follows:

"Article 84. Evidence

1. In criminal proceedings, evidence is factual knowledge, which has been obtained in a procedure prescribed in the present Code on grounds of which investigator, public prosecutor, investigating judge and court establish the presence or absence of facts and circumstances which are important for the criminal proceedings and are subject to be proved.
2. Evidence can be collected in physical or electronic form. Procedural sources of evidence are testimonies, objects, documents, expert findings.".

2) Chapter 4 sub-chapter 4 "§ 4. Physical evidence and documents" should be amended as follows:

"§ 4. Physical evidence, electronic evidence and documents".

3) Articles 98[1] and 100[1] should be inserted as follows:

Article 98[1]. Electronic evidence

1. Electronic evidence means evidence that can be collected in electronic form of a criminal offence.

2. Electronic evidence is derived from electronic devices, data storage mediums, as well as from computer networks, including the Internet and its applications. The information it contains does not possess an independent physical form.
3. Electronic evidence may be presented and examined also as exhibits (*alt:* objects) and documents.

Article 100[1]. Custody of electronic evidence

The seizure of electronic evidence takes place by producing an exact copy of the specific data or of the whole content of the storage medium. If producing a copy is not possible or there is a concern that the data sought would otherwise be lost, the storage medium containing electronic evidence is seized.

Explanatory note:

The Budapest Convention does not provide for a definition of electronic evidence. However, in order to implement Articles of the Convention on procedural measures, defining it would be an option. This can be achieved by introducing a specific definition of electronic evidence in the Code of Criminal Procedure (CPC), or by amending general definition of evidence to that it stipulates with necessary precision and foreseeability that evidence in electronic form is covered by its scope.

The CPC does not contain the definition of electronic evidence. Like many other countries, Ukrainian CPC and its rules on evidence are based on a traditional, general notion of evidence. According to Article 84(1) of the CPC, evidence is defined broadly, and covers any factual knowledge, obtained in accordance with the CPC, by which presence or absence of facts and circumstances which are important for criminal proceedings can be proven. Sources of such knowledge (evidence) can be testimonies, objects, documents and expert findings.[3] As the current article provides for an exhaustive list, it does not leave room for interpretation.

According to Article 99(1), a 'document' is "material object, which was created specifically for conservation of information, such object containing fixed by means of written signs, sound, image etc. the knowledge that can be used as evidence of the fact or circumstance which is established during criminal proceedings". It is further stipulated in paragraph 2 that documents might be "materials of photography, sound recording, video recording and other data media (including electronic)".

Although sometimes general rules on evidence may cover and could be applied to information stored in electronic form, it does not appear to be a completely satisfactory solution in the Ukrainian CPC. While it seems that there might be an opportunity to use electronic information as evidence if it is stored on data media on the basis of Article 99(2), not all types of electronic evidence could be considered as 'documents'.

Opinions of Ukrainian stakeholders are divided about whether specific a definition of 'electronic evidence' is necessary. However, discussions with relevant authorities showed that there is some uncertainty regarding the application of Articles 84 and 99.

The purpose of the amendments is to introduce a specific definition on electronic evidence that would cover digital information from different computer systems, their peripherals other

[3] CPC, Article 84(2).

electronic devices as well as digital information from data storage mediums and from the computer networks including the Internet.

In addition, introduction of a definition is accompanied by a provision on accessing and custody of the information that would be used as evidence in criminal proceeding.

Firstly, introducing such definition would make drafting specific procedural measures much easier. This is particularly important because the rest of the CPC rules on evidence are not in line with the concept of electronic evidence, as all existing procedural measures refer to evidence as physical or tangible object. Secondly, introducing the notion of 'electronic evidence' would increase legal clarity and foreseeability of the law.

Specific legislation on electronic evidence and related procedural measures would enable to establish rules on the admissibility of electronic evidence.

The use of a definition of electronic evidence may necessitate amendments to procedural measures in several articles of the Procedural Code. For example, the following additional changes may be considered:

Article 93 (1)– Collection of evidence

Collection of evidence is carried out by parties to criminal proceedings, victim and representative of a legal person in whose respect proceedings are taken in accordance with the procedure laid down in by the present Code. **In all following situations, the evidence may be in the form of testimony, from witnesses and experts, physical evidence, such as documents and objects and electronic evidence, which is described in Articles 84, 98 and 100. It is the responsibility of the party introducing the evidence to ensure that it has not been altered or changed in any way and that its integrity has been maintained throughout.**

Article 93 (2, 3) would not need amending, except for sub paragraph (2) of the third paragraph of Article 93, as amended by Law # 314-VII of 25.03.2013}

The evidence, in all forms described above, may be obtained from a foreign state within the framework of international cooperation in the course of criminal proceedings.

Article 94 – Evaluation of Evidence

Investigator, public prosecutor, investigating judge, court evaluates evidence based on his own moral certainty grounded in comprehensive, complete, and impartial examination of all circumstances in criminal proceedings being guided by law, evaluates any evidence from the point of view of adequacy, admissibility, and in respect of the aggregate of collected evidence, sufficiency and correlation, in order to take a proper procedural decision. **In cases where electronic evidence is present, specific care should be taken to ensure that proper procedures have been followed such that the integrity of the evidence, from the point of seizure to the presentation in court, has been maintained and can be validated.**

Article 100 – Custody of physical evidence (partial)

A document shall be kept throughout all criminal proceedings. Upon request of the owner of a document, investigator, public prosecutor, court may issue a copy of this document, and if necessary, the original, attaching to the criminal proceedings certified copies thereof in their

stead. **In cases where electronic evidence is present, an exact copy of the contents of any electronic devices may take the place of a copy of a physical object or document.**

2.3 Expedited preservation and provisional disclosure of stored computer data

In order to give effect to Articles 16 and 17 of the Convention, new Article 245[1] should be added, with the following text:

Article 245[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 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 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. 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 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.
5. Taking into account the volatile nature of electronic evidence and risks of loss or alteration, the investigator/prosecutor can serve the ruling noted in this Article in electronic format."

Explanatory note:

It follows from the text of the Articles 16 and 17 of the Convention, its Explanatory report[4], as well as reports adopted by the Cybercrime Convention Committee (T-CY)[5], that there are

[4] Explanatory report, para. 160.

essentially two methods of ensuring compliance with these provisions. The first, and the preferred one, is for a Party to introduce specific preservation order in its domestic legislation. The alternative, which is based upon the phrase "similarly obtain" in Article 16(1), is to use production order or search and seizure mechanism to expeditiously gain possession of data.

Ukraine did not implement Articles 16 and 17 of the Convention by introducing specific preservation order. Although Chapter 15 of the Criminal Procedure Code foresees some possibility of preserving computer data by using 'provisional access to objects and documents', this possibility was considered insufficient. Therefore, legislative amendments were considered necessary in order to give full effect to the provisions of the Convention. In such circumstances, experts are of the opinion that introduction of the standalone preservation order would be highly desirable. Consequently, new Article 245[1] is proposed.

Draft text of this new article takes account of the following:

- To ensure full compliance with Article 16 when introducing specific preservation order, national legislation should ensure that preservation order is applicable for any computer data, including traffic data, content data and subscriber information. This requirement is explicitly elaborated in paragraph 2 of the proposed article.
- The scope of application of preservation order should be not be limited in relation to criminal offences. No such limitation is present in the text, nor does it follow from other provisions of the CPC.
- A preservation order should be applicable against any legal or natural person (including, but not limited to, service providers) who possesses or controls data. This is elaborated in the paragraph 1 of the proposed article.
- Preservation order should have limited duration, "for a period of time as long as necessary, up to a maximum of ninety days", and the Party should be allowed to introduce the possibility of renewing the order. These requirements are elaborated in paragraph 1 of the proposed article.
- 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". This requirement is given effect in the paragraph 3 of the proposed article.
- Preservation order should 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 future. This follows from the text of paragraph 1, which implies that only existing computer data (data in someone's possession or under someone's control) are subject to preservation order.

As regards conditions and safeguard applicable to a preservation order, it was noted by the Cybercrime Convention Committee that those "should not be too restrictive or complex". Instead, focus is on the requirement that preservation be possible in an expedited manner.

In the experts' opinion, the proposed article 245[1] observes general principles regarding quality of the law (precision and foreseeability of the law). Judicial oversight over the issuing of preservation order is not mandatory, since such measure interferes only in the slightest possible manner with the interests of person who is required to preserve data. On the other

[5] See in particular *Implementation of the preservation provisions of the Budapest Convention on Cybercrime*, Assessment report adopted by the T-CY at its 8th Plenary (5-6 December 2012) (hereinafter: Preservation provisions report 2012; Also Supplementary report adopted by the 13th Plenary of the T-CY (15-16 June 2015)

hand, preserved data should be made available to the authorities only on the basis of production order, or seizure, both of which are subject to more extensive conditions and safeguards.

2.4 Production Order

In order to give effect to Article 18 of the Convention, the following amendments are proposed:

Article 160. Motion to grant provisional access to objects and documents

1. Parties to criminal proceedings may apply to investigating judge during pre-trial investigation or to court during trial, for granting provisional access to objects and documents of criminal proceedings, except those specified in Article 161 of the present Code. Investigator may submit such motion upon approval of public prosecutor.

2. By prosecutor's motion, the court shall issue the ruling obliging:

1) any 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;

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

3. Where there are grounds to believe that subscriber information, as defined in par. 2 Article 245^1 of this Code, is held by a service provider offering its services in the territory of Ukraine to submit subscriber information relating to such services in that service provider's possession or control, the prosecutor/investigator can issue a ruling ordering service provider to submit subscriber information without court's ruling referred to in par. 1 of this Article. Taking into account the volatile nature of electronic evidence and risks of loss or alteration, the investigator/prosecutor can serve the ruling noted in this paragraph in electronic format.

4. A service provider for the purposes of this Article shall mean an electronic communications service provider defined by the Law of Ukraine "On Electronic Communications."

5. A motion shall contain:

1) brief description of circumstances of the criminal offense in connection with which the motion is filed;

2) legal qualification of the criminal offense under Ukrainian law on criminal liability indicating the article (paragraphs of article);

3) objects and documents the provisional access to which is planned to be granted; including those held in electronic format, having been derived from devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras and other portable equipment (including data storage devices), as well as from the Internet. The information contained in these devices, does not possess an independent physical form.

4) grounds to believe that the objects and documents are or can be in possession of the physical or legal person concerned;

5) significance of the objects and documents for establishing circumstances in the criminal proceedings concerned;

6) possibility to use as evidence the information contained in the objects and documents, and impossibility to otherwise prove circumstances which are supposed to be proved with

the use of such objects and documents, in case the motion to grant provisional access pertains to objects and documents containing secrets protected by law;

7) substantiation of the necessity to seize the objects and documents, if such an issue is raised by a party to criminal proceedings.

Article 161. Objects and documents to which access is prohibited

Objects and documents, **whether held in physical or electronic form,** to which access is prohibited shall include:

1) correspondence or any other form of communication between defense counsel and his client or any person, who represents his client, in connection with the provision of legal assistance;

2) objects which are attached to such correspondence or any other form of communication.

Article 162. Objects and documents containing secrets protected by law

Secrets protected by law and contained in objects and documents, **whether held in physical or electronic form**, are:

1) information in possession of a mass medium or a journalist and which was provided to them on condition that its authorship or source of information would not be disclosed;
2) information, which may constitute medical secret;
3) information which may constitute secrecy of notary's activity;
4) confidential information, including commercial secrets;
5) information which may constitute bank secrecy;
6) personal correspondence of a person and other notes of personal nature;
7) information held by telecommunication operators and providers on communications, subscriber, rendering of telecommunication services including on receipt of services, their duration, content, routes of transmission etc.[6];
8) personal data of an individual, which are in his personal possession or in personal database, which the possessor of personal data has;
9) State secret.

Article 163. Consideration of the motion for provisional access to objects and documents

1. After having received motion for provisional access to objects and documents, **including those in both physical and electronic form**, investigating judge, court shall summon the person who possesses such objects and documents, with the exception of the case specified in part two of this Article.

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

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

4. Investigating judge, court shall consider the motion with participation of the party to criminal proceedings which filed the motion, and the person who possesses the objects and

[6] Including this information as secret, appears to preclude the possibility of its access during the reinvestigation phase. This requires deletion from the provisions of Article 162.

documents, except as provide otherwise by the second paragraph of this article. Non-compliance with court summons of a person who possesses the objects and documents, without valid reasons, or his failure to inform of the reasons for non-appearance, shall not be obstacle for considering the motion.

5. Investigating judge, court shall issue the ruling to grant provisional access to objects and documents if the party to criminal proceedings proves in its motion the existence of sufficient grounds to believe that the objects or documents:

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

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

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

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

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

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

Article 164. Ruling on the provisional access to objects and documents

1. Investigating judge's, court's ruling on the provisional access to privileged objects and documents, **in both physical an electronic form**, shall include:

1) last name, first name, and patronymic of the person who is granted provisional access to objects and documents;

2) date of ruling;

3) statutory provision under which the ruling has been passed;

4) last name, first name, and patronymic of the physical person or name of the legal person that shall grant provisional access to objects and documents;

5) name, description, other information which make it possible to identify objects and documents, to which access should be granted;

6) order to grant (ensure) provisional access to objects and documents to the person specified in the ruling, and to provide him the opportunity to seize the objects and documents concerned if a respective decision has been adopted by investigating judge, court; **in cases where objects and documents are held in electronic format, investigative judge may order the seizure of the devices containing the information, only where taking a digital copy will interfere with the administration of justice. In all other cases the order should allow the taking of an exact copy of the ordered data;**

7) period of validity of the ruling, which may not exceed one month of the date of its issuance;

8) statutory provisions, which establish implications of a failure to comply with the ruling of the investigating judge or court.

Article 165. Execution of the investigating judge's or court's ruling on the provisional access to objects and documents

1. The person named in investigating judge's, court's ruling on provisional access to objects and documents as the possessor of objects and documents shall be required to give provisional access to objects and documents, **in physical or electronic form**, specified in the ruling to the person indicated in the investigating judge's, court's ruling.
2. The person indicated in the investigating judge's, court's ruling shall be required to produce the original, and hand over a copy, of the investigating judge's, court's ruling on provisional access to objects and documents to the person named in the ruling as the possessor of the objects and documents.
3. The person who produces investigating judge's, court's ruling on provisional access to objects and documents shall be required to leave the list of objects and documents, which have been seized based on investigating judge's, court's ruling, with the possessor of objects and documents.
4. Upon demand of possessor, the person who produces the ruling on provisional access to objects and documents, shall be required to leave copies of seized documents. Copies of seized documents shall be made using copying equipment, electronic means of the possessor (upon his consent) or copying equipment, electronic means of the person who produces the ruling on provisional access to objects and documents.

Explanatory note:

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. 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.

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: "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 are 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.

CPC of Ukraine provides only very limited possibility to order production of data using provisions on 'provisional access to documents'. The main concern is that application of this measure is unnecessarily burdened by imposing high thresholds in the form of conditions and safeguards which are applicable. This is particularly true for subscriber information. There are two issues here. Firstly, as explained above, the notion of 'information held by telecommunication operators on … subscribers' is not elaborated in the law. This is not acceptable from the point of certainty and foreseeability of law. Secondly, such information are deemed 'secrets protected by law' and are subject to unnecessarily extensive conditions and safeguards.

2.5 Search and Seizure

In order to give effect to Article 18 of the Convention, the following amednments are proposed:

Article 233. Entering home or any other possession of a person

1. Nobody is allowed to enter home or any other possession of a person for any purpose whatsoever otherwise than upon voluntary consent of the owner or based on a ruling of investigating judge, and except in cases specified in part three of this Article.
2. It is understood that "home" means any premise an individual owns permanently or temporarily whatever purpose it serves and whatever legal status it has, and adapted for permanent or temporary residence of physical persons, as well as all constituent parts of such premises. Premises specially intended for keeping of persons whose rights have been restricted by law, are not deemed dwellings. "Other possession of a person" refers to a vehicle, land parcel, garage, other structures or premises for household, service, business, production or other use etc., which a person owns.
3. The investigator, public prosecutor shall have the right, before the investigating judge's ruling, to enter home or any other possession of a person only in urgent circumstances related to saving human life and property, **including information held in electronic format**, or in a hot pursuit of persons suspected of committing a crime. In such a case, the public prosecutor or investigator, with approval of the public prosecutor, shall be required to file promptly after such actions a motion with the investigating judge for a search warrant. The investigating judge shall consider such motion under the rules of Article 234 of this Code, having verified inter alia whether there did exist grounds for entering home or other possession of the person without a ruling of the investigating judge. Where the public prosecutor refuses to approve the motion for search or the investigating judge dismisses the motion for search, evidence found as a result of such search shall be inadmissible and any information so obtained shall be subject to destruction as provided under Article 255 of this Code.

Article 234. Search

1. A search is conducted with the purpose of finding and fixing information on circumstances of commission of criminal offense, finding tools of criminal offense or property obtained as a result of its commission, as well as of establishing the whereabouts of wanted persons.
2. A search shall be based on investigating judge's ruling.
3. Whenever it is necessary to conduct a search, investigator with approval of public prosecutor, or public prosecutor shall submit an appropriate request to investigating judge containing the following information:

1) designation and registration number of criminal proceedings;
2) brief description of circumstances of the criminal offense in connection with investigating which the request is submitted;
3) legal qualification of the criminal offense indicating Article (Article part) of the Ukrainian law on criminal liability;
4) grounds for search;
5) home or any other possession of a person or a part thereof or other possession of the person where the search should be conducted;
6) person who owns the home or other possession, and person in whose actual possession it actually is;
7) objects, documents, **electronic evidence** or individuals to be found,

The request shall be required to be attached originals or copies of documents and other materials by which public prosecutor, investigator substantiates the arguments of the request, as well as an extract from the Integrated Register of Pre-Trial Investigations related to the criminal proceedings in the framework of which the request is submitted.

4. A request for search shall be considered in court on the day of receipt, with participation of investigator or public prosecutor.
5. Investigating judge shall reject a request for search unless public prosecutor, investigator proves the existence of sufficient grounds to believe that:

1) a criminal offense was committed;
2) objects and documents to be found are important for pre-trial investigation;
3) knowledge contained in objects and documents being searched may be found to be evidence during trial;
4) objects, documents or persons to be found are in the home or any other possession of a person indicated in the request.

Article 235. Ruling to authorize a search of home or any other possession of a person

1. Investigating judge's ruling authorizing search of home or other possession of a person on grounds provided in public prosecutor's, investigator's request, shall give the right to enter home or other possession of a person only once.
2. Investigating judge's ruling authorizing search of home or other possession of a person shall be required to comply with general requirements for court decisions laid down in the present Code as well as contain information on the following:

1) term of effect of the ruling which may not exceed one month after the day it was passed;
2) public prosecutor, investigator who requests the search;
3) legal provision based on which the ruling is passed;
4) home or any other possession of a person or a part thereof, or other possession of the person where the search should be conducted;
5) person who owns the home or other possession, and person in whose actual possession it actually is;

6) objects, documents, **electronic evidence** or individuals to be found. **Where electronic evidence is found, judge's ruling may specify if the seizure of the data carrying device is necessary or if a copy of the data will be sufficient. The public prosecutor, investigator may make representation on the preferred method, 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.**

3. Two copies of the ruling should be prepared and expressly marked as copies.

Article 236. Execution of the ruling to authorize search of home or any other possession of a person

1. Investigator or public prosecutor may execute the ruling to authorize a search of home or any other possession of a person. The victim, the suspect, defense counsel, representative, and other participants to criminal proceedings may be invited to attend. Whenever investigator, public prosecutor needs assistance in issues requiring special knowledge, they may invite specialists to participate in the search. The investigator, public prosecutor shall take adequate measures to ensure that persons whose rights and legitimate interests may be abridged or violated are present during such search.
2. A search of home or other possession of a person based on investigating judge's ruling should be conducted in time when the least damage is caused to usual occupations of their owner unless the investigator, public prosecutor finds that meeting such requirement can seriously compromise the objective of the search.
3. Prior to the execution of investigating judge's ruling, the owner of home or any other possession or any other present individual in case of the absence of the owner, should be produced court's ruling and given a copy thereof. Investigator, public prosecutor may prohibit any person from leaving the searched place until the search is completed and from taking any action which impede conducting search. Failure to follow these requests entails liability established by law.
4. If no one is present in the home or other possession, the copy of ruling should be left visible in the home or other possession. In such a case, investigator, public prosecutor is required to ensure preservation of property contained in the home or any other possession and make it impossible for unauthorized individuals to have access thereto.
5. Search based on court's ruling should be conducted within the scope necessary to attain the objective of search. Upon decision of the investigator, public prosecutor, individuals present in the home or other possession may be searched if there are sufficient grounds to believe that they hide on their person objects or documents which are important for criminal proceedings. Such search should be conducted by individuals of the same sex.
6. During the search, investigator, public prosecutor shall have the right to open closed premises, depositories, objects if the person present during the search, refuses to open them, or if the search is conducted in the absence of persons specified in part three of this Article. **If, during the search, investigator, public prosecutor search or similarly access a specific computer system or part of it, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, investigator, prosecutor shall be able to expeditiously extend the search or similar accessing to the other system.**
7. During the search, investigator, public prosecutor may conduct measurements, shoot pictures, make audio or video recording, draw plans and schemes, produce graphic images of

the searched home or other possession of a person, or of particular objects, make prints and moulds, inspect and seize objects and documents which are important for criminal proceedings. Objects seized by law from circulation shall be subject to seizure irrespective of their relation to the criminal proceedings concerned. Seized objects and documents not included in the list of those directly allowed to be found in the ruling authorizing the search, and are not among objects withdrawn by law from circulation, shall be deemed provisionally seized property.

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

9. Persons who are present at the search may 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 237. Inspection

1. Investigator, public prosecutor shall carry out visual inspection of the area, premises, items and documents to find and record the information relating to the commission of a criminal offence.

2. Inspection of home or any other possession of a person shall be done in accordance with rules of the present Code governing the search of home or any other possession of a person.

3. The victim, suspect, defense counsel, legal representative and other participants to criminal proceedings may be invited to take part in the inspection. In order to have assistance in matters requiring special knowledge, investigator, public prosecutor may invite specialist to participate in the inspection.

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

5. During inspection, it shall be allowed to seize only objects and documents of importance for the pre-trial investigation, and objects withdrawn from circulation. All objects and documents which have been seized are subject to immediate inspection and sealing with signed acknowledgement by participants to the inspection. If it is impossible to inspect objects and documents on the premises or if their inspection is complicated, they shall be temporarily sealed and stored as they are until final inspection and sealing thereof is made. Where the material to be seized is believed to be held in electronic format on a computer or similar device, prosecutor, an **investigator may seize or similarly secure for later inspection, 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. Where seizure instead of on-site inspection is enacted, prosecutor, inspector should make a written record of the reason for this decision and make it available as part of the official search record. Prosecutor, inspector may take representation from persons present, including, victim, suspect, defence counsel, legal representative and other participants, as to why onsite inspection and not seizure of data carriers should be undertaken. A record of the representations and subsequent decision should be recorded in the search record.**

6. Investigator, public prosecutor may prohibit any individual from leaving the inspected place till the completion of inspection and from committing any actions which impede inspection. Failure to comply with such requests entails liability under law.

7. During inspection, investigator, public prosecutor or upon their assignment, the invited specialist may carry out measurements, photographing, audio or video recording, draw up plans and schemes, prepare graphical images of the place or particular objects, produce

prints and moulds, examine and seize objects and documents of importance for criminal proceedings. Objects seized from circulation by law shall be subject to seizure irrespective of their relation to criminal proceedings. Seized objects and documents which are not objects seized from circulation by law shall be deemed provisionally seized property.

Explanatory note:

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, national legislation should ensure the following:

Purpose of article 19: Enable authorities to (1) conduct measure of search of similar accessing, (2) expeditiously extend such measure to linked systems, (3) seize computer system, mediums or data and (4) order any person who has knowledge or information necessary to conduct search to provide them.

Scope of power to search: competent authorities must be able to search or similarly access (1) computer system, (2) parts of computer systems, (3) storage mediums and (4) computer data stored therein.

Power to extend search: competent 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.

Power to request information necessary to conduct search: Competent 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.

Scope of power to seize data: Competent authorities must be empowered to seize or similarly secure computer data, which includes powers to (1) seize (take away) or similarly secure computer system, parts of it or storage mediums, (2) make and retain a copy of computer data; (3) maintain the integrity of the relevant stored computer data; and (4) render inaccessible or remove those computer data in the accessed computer system.

Conditions and safeguards: National legislation should observe general principles regarding quality of the law. It may exclude privileged data or information from the scope of search / seizure. Grounds justifying application should be elaborated. Judicial or other independent supervision should be exercised.

Search and seizure of computer data can partially be achieved on the basis of Chapter 16 ('provisional seizure of property'), search of home or other possessions of a person (Articles 234 – 236), Articles 234 – 236 of the CPC (search) and 167 ('provisional seizure of property') can in principle be used to achieve some purposes of Convention's Article 19. However, there are several shortcomings if these provisions are to be applied on search and seizure of computer data.

Firstly, these provisions were meant to be used with regard to tangible objects. This is visible firstly from the object of these actions, which is 'property' or 'possessions'. While this includes the notion of 'documents', it is necessary to once again point to the limited scope of that notion. Moreover, measures which are specific to search and seizure of computer data

are not implemented. Also, in the context of search, there is no provision which would enable continuing search online (extension of search to connected systems).

Chapter 21 of the Criminal Procedure Code provides for the possibility to conduct covert investigative actions (special investigation techniques) and gives a list of different measures. Here the main concern is that the measures indicated are only applicable in case of serious crime and therefore might not include necessarily all the cybercrime offences. Article 264 which provides the possibility to collect data from electronic information systems enables law enforcement authorities to access computer system and obtain information which can be considered as electronic evidence. Together with Article 256 the results of such an action can be used as evidence.

Bearing in mind the assessment given above it is possible to conclude that Article 19 of the Convention has been partially implemented. Criminal Procedure Code enables search and seizure as well as obtaining information from a computer system. Although it is not explicitly mentioned it is possible to conclude that covert access without the knowledge of the owner to a computer system could cover also the extended online search. Still recommendation would be to have a clear reference to that, because it might not be sufficient in case of ordinary search and seizure which might take place with the awareness of the owner. In addition legislation needs to be improved with regard to the copying of the data and making it inaccessible.

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

Articles 20 and 21 of the Convention provide for two procedural powers which directly restrict the rights to the protection of private life and personal data. Initial analysis of the Ukrainian legislation indicated that legislative provisions governing these powers might not be completely in line with the Council of Europe's legal framework. Therefore, in the 2016 Report the following recommendation was made:

Review the limitations and safeguards for the application of monitoring and interception provisions pursuant Art. 20 and 21 of the Convention, especially with regard to detailed requirements developed in the case-law of the ECtHR.

What follows is a series of proposed amendments in Chapter 21 of the Ukrainian CPC, which governs "interference in private communication" (text marked in blue). Explanations are provided for articles affected by these amendments.

Chapter 21. Covert Investigative (Detective) Actions
§ 1. General provisions related to covert investigative (detective) actions

Article 246. Grounds for covert investigative (detective) actions

1. Covert investigative (detective) actions are a type of investigative (detective) actions the information on the fact and methods in which they are conducted may not be disclosed, except as prescribed in the present Code.
2. Covert investigative (detective) actions are conducted if information on criminal offence and its perpetrator cannot be obtained otherwise. **Unless specified otherwise in this Chapter,** covert investigative (detective) actions specified in Articles 260, 261, 262, 263, 264 (in part of actions based on the investigating judge's ruling) 267, 269, 270, 271, 272 and 274 of the present Code, as well as those the decision to conduct which are taken by

investigating judge, shall be conducted exclusively in criminal proceedings in respect of grave crimes or crimes of special gravity.
3. Investigator, public prosecutor, and investigating judge in cases specified by the present Code, upon request of public prosecutor or upon request of investigator approved by public prosecutor, shall take decision on the conducting of covert investigative (detective) actions. Investigator shall be required to inform public prosecutor on the decision to conduct certain covert investigative (detective) actions and their results. Public prosecutor may prohibit or stop the conducting of covert investigative (detective) actions.
4. Only public prosecutor is vested the right to take decision to conduct such a covert investigative (detective) action as control over the commission of crime.
5. Decision to conduct a covert investigative (detective) action shall state the time limit for its conduct. Time limit for the conducting of a covert investigative (detective) active may be extended:
by public prosecutor, if the covert investigative (detective) action is conducted by his decision, up to eighteen months;
by head of pre-trial investigative agency, if the covert investigative (detective) action is conducted by his or investigator's decision, up to six months;
by the head of a stand-alone Directorate of the Ministry of Internal Affairs of Ukraine;
by head of the Security Service of Ukraine's chief, separate office; by the head of a relevant unit of the National Anti-Corruption Bureau of Ukraine and the State Bureau of Investigations;
by head of the Ministry of Internal Affairs of Ukraine's chief office, office and of the agency carrying out supervision over the compliance with tax legislation, an agency under the State Bureau of Investigations in the Autonomous Republic of Crimea, oblasts, cities of Kyiv and Sevastopol;
by head of the Security Service of Ukraine's regional body within their competence, if the covert investigative (detective) action is conducted by investigator's decision, up to twelve months;
{The fourth sentence of Paragraph 5 of Article 246 as amended by Law № 1698-VII of 14.10.2014} by the Minister of Internal Affairs of Ukraine, the Head of the Security Service of Ukraine, the Director of the National Anti-Corruption Bureau of Ukraine, the head of the central executive authority supporting the development and implementing tax and customs policy and chief of the State Bureau of Investigations, if the covert investigative (detective) action is conducted by investigator's decision, up to eighteen months;{The fifth sentence of Paragraph 5 of Article 246 as amended by Law #406-VII of 04.07.2013 and by Law № 1698-VII of 14.10.2014 }
by investigating judge, if the covert investigative (detective) action is conducted by his decision, as prescribed by Article 249 of the present Code.
6. The right to conduct covert investigative (detective) actions is vested in the investigator who conducts pre-trial investigation of a crime, or on his assignment, in the competent operative units of bodies of internal affairs, bodies of security, of the National Anti-Corruption Bureau of Ukraine, the State Bureau of Investigations, bodies supervising compliance with the tax and customs legislation, bodies of the State Penitentiary Service of Ukraine, and bodies of the State Border Guard Service of Ukraine . Upon investigator's or public prosecutor's decision, other persons may also be engaged in the conducting of covert investigative (detective) actions.{Paragraph 6 of Article 246 as amended by Law # 406-VII of 04.07.2013 and by Law № 1698-VII of 14.10.2014}

Explanatory note:

Change in paragraph 2 is necessary to open the possibility of creating specific rules governing material scope of interception order (Article 263 paragraph 2).

Article 248. Examination of the request to obtain permission for the conducting of a covert investigative (detective) action

1. Investigating judge is required to consider the request to obtain permission for the conducting of a covert investigative (detective) action within six hours after he has received such request. The request shall be considered with participation of the person who filed the request.

2. The request shall contain:

1) designation and registration number of the criminal proceedings concerned;

2) brief description of the circumstances of the crime within the framework of investigation of which the request is filed;

3) legal qualification of the crime with indication of Article (section of Article) of the Criminal Code of Ukraine;

4) information on the individual (individuals), place or object in whose respect it is necessary to conduct covert investigative (detective) action;

5) circumstances that provide grounds for suspecting the individual of committing the crime;

6) type of covert investigative (detective) action to be conducted, and substantiation of the time limits for the conducting thereof;

7) substantiation of impossibility to obtain otherwise knowledge on crime and the individual who committed it;

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

9) substantiation of the possibility to obtain in the course of conducting of covert investigative (detective) action, of evidence which, alone or in concurrence with other evidence, may be significantly important for the clarification of the circumstances of crime or the identification of perpetrators thereof.

Investigator's, public prosecutor's request shall be attached an extract from the Integrated Register of Pre-Trial Investigations pertaining to the criminal proceedings within the framework of which the request is filed.

3. Investigating judge passes a ruling to allow conducting the requested covert investigative (detective) action if the public prosecutor proves that sufficient grounds exist that:

1) a crime of relevant severity has been committed;

2) in the course of covert investigative (detective) action, information is likely to obtained, which alone or in totality with other evidence may be of essential importance for establishing circumstances of the crime or identification of perpetrators thereof;

3) it is impossible to obtain otherwise knowledge on crime and the individual who committed it.

4. Investigating judge's ruling to allow conducting a covert investigative (detective) action should meet general requirements for judicial decisions as prescribed in the present Code, as well as contain information on:

1) reasons why the purpose of investigation cannot be achieved by other, less intrusive, means;

2) public prosecutor, investigator who applied for permission;

3) criminal offence which is subject of pre-trial investigation within which the ruling is passed;

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

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

6) time in which the ruling is valid.

5. The ruling rendered by investigating judge to give no permission to conduct covert investigative (detective) action shall not impede filing a new motion to obtain such permit.

Explanatory note:

Adequate reasoning showing the necessity to conduct covert investigative (detective) actions is an important safeguard against abuse. Therefore, the CPC should explicitly require that such reasoning is present in both the prosecutor's request and the investigating judge's ruling.

Article 250. Conducting a covert investigative (detective) action before investigating judge adopts a ruling

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

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

3. **If the investigating judge passes a ruling denying permission to conduct the covert investigative (detective) action concerned, or if he does not issue a ruling within twenty-four hours,** carrying out any activities related to conducting a covert investigative (detective) action should be immediately discontinued. Information obtained as a result of conducting such covert investigative (detective) action **must be destroyed immediately,** in accordance with Article 255 of the present Code.

Explanatory note:

The proposed changes seek to add legal clarity and foreseeability, as well as to introduce additional safeguards in the text of the CPC. Most importantly, it is necessary to ensure that any material obtained without authorization is destroyed without delay.

Article 253. Notifying individuals in whose respect covert investigative (detective) actions have been conducted

1. Individuals whose constitutional rights were temporarily restricted during conducting covert investigative (detective) actions, as well as the suspect, his/ her defense counsel shall be informed about such restriction in written form by public prosecutor or, upon his instruction, by investigator, **as soon as that is possible without jeopardizing the purpose of the measure.**

2. Specific time of notification shall be chosen taking into account the presence or absence of possible risks for the attainment of the objective of pre-trial investigation, public security, life or health of individuals who are involved in the conduct of covert investigative (detective) actions. Appropriate notification of the fact and results of covert investigative (detective) actions shall be required to be made within twelve months since the date of termination of such actions, but not later than an indictment has been produced to court.

Explanatory note:

Proposed changes seek to maintain appropriate safeguard, while at the same time specifying conditions under which obligation to notify should be applicable.

§ 2. Interference in private communication

Article 258. General provisions related to interference in private communication

1. Nobody may be subjected to interference in private communication without investigating judge's ruling.
2. Public prosecutor, investigator upon approval of public prosecutor shall be required to apply to investigating judge for permission to interfere in private communication as prescribed in Articles 246, 248-250 of the present Code, if any investigative (detective) action implies such interference.
Whenever investigating judge passes the ruling to deny interference in private communication, public prosecutor, investigator may file a new request only with new information.
3. Communication is transmitting information in any way from one person to another directly or using any connection. Communication is considered to be private insofar as information is transmitted and stored under such physical or legal conditions where participants to the communication can expect that such information is protected from interference on the part of others.
4. Interference in private communication implies access to the contents of communication under conditions when participants to the communication can reasonably expect that their communication is private, **and also access to the information about communication (traffic data).** The following shall be types of interference in private communication:

1) audio, video monitoring of an individual;
2) arrest, examination and seizure of correspondence;
3) **surveillance and interception of communication content data;**
4) collecting information from electronic information systems;
5) accessing and analysing information about communication (traffic data).

5. Interference in private communication of defense counsel, between clergyman and the suspect, accused, convict, acquitted shall be forbidden.

Explanatory note:

Section 2 of Ukrainian CPC's Chapter 21 regulates "interference in private communication", which includes several covert (detective) investigative actions (CDIA). Analysis of Ukrainian legislation showed that it is at least not certain whether this section applies to real-time collection of traffic data, as defined in Article 20 of the Cybercrime Convention. While the text of Articles 263 and 264 might allow such interpretation, Article 258(4) nevertheless stipulates that "interference in private communication implies access to the contents of communication". In the light of these provisions, experts consider it necessary to differentiate clearly between surveillance and interception of communication content data (para 4/3) and accessing and analysing information about communication (traffic data) (para 4/5). At the same time, measure of "Collecting information from transport telecommunication networks" (article 263) shall not be necessary if proposed changes are implemented.

The text of the current Article 263 should be completely amended, as follows:

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

~~1. Collecting information from transport telecommunication networks (networks which provide transmitting of any signs, signals, written texts, images and sounds or messages between telecommunication access networks connected) is a variety of interference in private communication conducted without the knowledge of individuals who use telecommunication facility for transmitting information based on the ruling rendered by the investigating judge, if there is possibility to substantiate the facts during its conducting, which have the importance for criminal proceedings.~~

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

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

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

Proposed revised text:

Article 263. Surveillance and interception of communication content data

1. Surveillance and 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 investigating judge.

2. Surveillance and 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 grave crime, crime of special gravity or one of the crimes described in Chapter XVI of the Criminal Code. This measure can also be ordered against the person for whom is 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 stipulated in Article 248(4), investigating judge's ruling authorizing surveillance and 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. Surveillance and 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 investigating judge's ruling to the communication service provider concerned.

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.

Explanatory note:

Paragraph 1 makes in evident that Article 263 implies access to content data, and as such is differentiated from real-time collection of traffic data (Article 264.a).

Paragraph 2 introduces limitations of scope for interception order, in relation to criminal offences and persons against whom it can be applied.

Paragraph 3 seeks to ensure that interception orders are given only upon careful deliberation by the investigating judges.

Paragraphs 4 and 5 seek to ensure cooperation between law enforcement and service providers, while maintaining necessary safeguards (presentation of interception order, mandatory logging, supervision).

A new Article 264[1] should be introduced:

Article 264[1]. Accessing and analysing information about communication (traffic data)

1. Accessing and analysing information about person's communications is an interference with private communications conducted without the knowledge of individuals concerned. Information about communications includes all data which can be used to determine identity, duration and frequency of communications, as well as the location of communication device. For the avoidance of any doubt, this includes all "traffic data" a in Article 245[1] of this Code.
2. Accessing and analysing information about communication (traffic data) does not imply access to communication content data.
3. Accessing and analysing information about communication (traffic data) can only be executed upon written and reasoned ruling issued by the investigating judge, or if the person concerned gives his or her written consent.
4. 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 interceptions, and to make these records available to supervisory bodies.

Explanatory note:

Article 264[1] seeks to introduce a new procedural power of accessing and analysing information about communications, including traffic data, in real-time (paragraph 1). Measure is differentiated from analysis of content data (paragraph 2). It is mandatory that access to content and traffic data is subject to different procedural powers, since different conditions and safeguards are applicable. Judicial authorisation or voluntary consent is

required (para 3). Obligation to facilitate access, to maintain confidentiality and ensure logging for supervision purposes in specified in law (paragraph 4).

2.7 Optional recommendations not directly related to the Budapest Convention on Cybercrime

2.7.1 Amendments to the [Draft] Law on Electronic Communications

Currently, Article 48 of the Draft Law on Electronic Communications contains a very simple legal basis for data retention. Namely, according to Article 48 paragraph 10 *"Providers of electronic communications services shall: …10) keep records of electronic communications services within the limitation period specified by law and provide information on the provided electronic communications services in the order prescribed by law;…".*

This solution is insufficient, from the perspective of legal precision, foreseeability and proportionality.[7] Consequently, **and only if the decision is to maintain data retention obligations**, two new articles should be added, with the following text:

Article 48[1]. Data retention obligation

(1) Providers of electronic communications shall be obliged to retain electronic communications data referred to in Article 48[2] of this Law 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 Article 48[2] of this Law 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 referred to in paragraph 1 of this Article must retain data referred to in Article 48[2] for the period of twelve months from the date of the communication.
(4) Providers referred to in paragraph 1 of this Article 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:
1. 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;
2. 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;
3. access to retained data must be exclusively limited to authorised persons of competent bodies referred to in paragraph 1 of this article;

[7] 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.

4. 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 referred to in paragraph 1 of this Article must ensure at their own expense the implementation of all appropriate technical and organisational measures.
(7) The provider referred to in paragraph 1 of this Article must appoint a person responsible for the enforcement of measures and standards of information security.
(8) Providers referred to in paragraph 1 of this Article 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 referred to in paragraph 1 of this Article 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 referred to in paragraph 1 of this Article 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.

Article 48[2]. Categories of retained data

(1) The data retention obligation referred to in Article 48[1] of this Law shall include the following categories of data:

– data necessary to trace and identify the source of a communication;
– data necessary to identify the destination of a communication;
– data necessary to identify the date, time and duration of a communication;
– data necessary to identify the type of communication;
– data necessary to identify users' communication equipment or what purports to be their equipment;
– data necessary to identify the location of mobile communication equipment.

(2) The retained data referred to in paragraph 1 of this Article shall also refer to data relating to unsuccessful call attempts, whereby there is no obligation to retain data relating to unconnected calls.
(3) Data revealing the contents of the communication may not be retained.
(4) Detailed list of information about individual categories of retained data referred to in paragraph 1 of this Article shall be laid down in secondary legislation regulating the obligations of providers.

Explanatory note:

Proposed amendments reflect recommendations made in the 2016 Report, according to which:

i. The term 'records' should be defined. For reference, please see Article 5 of the EU Data Retention Directive. Complete list of categories of data to be retained can be defined in

secondary legislation, however it would be important to have at least general categories in the Law on Electronic Communications.

ii. It should be stipulated in law that content data must not be retained.

iii. Period for keeping 'records' should be stipulated in this law (instead of using phrase 'within the limitation period specified by law).

iv. It should be stipulated in the law that retained data (or 'records) must be deleted after the expiry of limitation period.

v. Law should specify the purposes for which retained data ('records') can be used. These purposes should be limited to the needs of crime investigation and prosecution, as well as those falling within the competence of security and intelligence agencies.

vi. It is not clear what is the relation between Article 48, para 1, subparagraph 10 and para 2 ('Providers of electronic communication services shall retain and provide the information on the provided electronic communications services to its subscriber in the order established by law'. This should be clarified.

vii. It should be stipulated in the law that providers shall keep records about performed search and rescue and undisclosed search operations, and that this information shall be made available only to competent supervisory bodies, at their request.

2.7.2 Proposal for secondary legislation in the field of data retention

A precise list of categories of data to be retained should be established in secondary legislation, passed on the basis of the new draft law (proposed article 48^2 para 4). It is proposed that the full list from Article 5 of the former EU Data Retention Directive[8] be used:

Article xx

Data to be retained on the basis of Articles 48^1 and 48^2 of the Law on Electronic Communications shall include the following:

(a) data necessary to trace and identify the source of a communication:
(1) concerning fixed network telephony and mobile telephony:
(i) the calling telephone number;
(ii) the name and address of the subscriber or registered user;
(2) concerning Internet access, Internet e-mail and Internet telephony:
(i) the user ID(s) allocated;
(ii) the user ID and telephone number allocated to any communication entering the public telephone network;
(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:
(1) concerning fixed network telephony and mobile telephony:

[8] This Directive was declared void by the European Court of Justice in 2014.

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

3 Conclusions

The proposals made by Council of Europe are submitted for consideration by the authorities of Ukraine.

The proposals of sections 2.1 to 2.6 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 2.7 are made in case the authorities of Ukraine 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.