



## Cybercrime legislation – country profile

### KOSOVO\*

*This profile has been prepared within the framework of the EU/COE Joint Project on Regional Cooperation against Cybercrime in South-eastern Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.*

Comments may be sent to:

Economic Crime Division  
Directorate General of Human Rights and Legal Affairs  
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506  
Fax: +33-3-9021-5650  
Email: [alexander.seger@coe.int](mailto:alexander.seger@coe.int)  
[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

Country/Area	Kosovo*
Signature of Convention:	No
Ratification/accession:	No
<b>Provisions of the Convention</b>	<b>Corresponding provisions/solutions in national legislation</b>

\* All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.

	<p><i>(pls quote or summarise briefly; pls attach relevant extracts as an appendix)</i></p> <p>The Republic of Kosovo has not ratified the Convention of the Council of Europe, given that it is not a member of the Council of Europe and member of UN, and as it is known the ratification of Conventions create rights and obligations between the parties. However, although the Republic of Kosovo has not ratified the Council of Europe conventions the entire national legislation is in harmony with these conventions. <b>The Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME</b> is adopted by the Assembly on 10th of June, 2010. (This law, drafted by local and international experts, is in compliance with European standards and the Budapest Convention)</p>
<p><b>Chapter I – Use of terms</b></p>	
<p><b>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”:</b>  For the purposes of this Convention:  a “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;  b “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;  c “service provider” means:  i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and  ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;  d “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</p>	<p><b>Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME</b></p> <p><b>Article 3 - Definitions</b>  1. Terms used in this law have the following meaning:  1.1. <b>Cyber crime</b> - a criminal activity carried out in a network that has as objective or as a way of carrying out the crime, misuse of computer systems and computer data.  1.2. <b>Computer system</b> - any device or device assembly interconnected or under an operative linkage, of which, one or more provide automatic data that are processed through computer programs;  1.3. <b>Automatic data processing</b> - a process by which the data are processed to the computer system through computer programs;</p>

1.4. **Computer program** - a group of instructions that may be implemented through a computer system in order to achieve certain results;

1.5. **Computer data** - any representation of facts, information or concepts in such a form that could be processed by means of computer systems. This category involves any computer program that may initiate computer systems to perform certain functions;

1.6. **Service provider** - any natural or legal person that provides an opportunity to users to communicate by computer system, and the person processing or collecting data for these providers of services and for users of services provided by them;

1.7. **Data on the traffic** - computer data concerning the *communication* that through a computer system and its output, representing part of the communication chain, indicating the origin of the communication, destination, line, time, date, size, volume and time duration as well as type of service used for communication;

1.8. **Data on users** - any information that may lead to identification of the user, including type of communication and service used, address of the post office, geographic address, IP address, telephone number or any other number of access and means of payment for pertinent services as well as any other information that may lead to identification of the user;

1.9. **Security measures** - refer to utilization of certain procedures, means or specialized computer program by means of which access to the computer system is limited or forbidden to a given category of users;

1.10. **Pornographic materials of minors** - refer to any material that presents a minor or an adult shown as minor of an explicit sexual behaviour or images

	<p>which, although it does not present a real person, simulates, in such credible way a minor with explicit sexual behaviour.</p> <p>1.11. <b>Interception</b> - obtaining, illegal seizure of the data from unauthorized persons.</p> <p><b>Article 4 - Unauthorized actions</b></p> <p>1. Pursuant to this Law, a person acts are considered unauthorized actions, if the person:</p> <p>1.1. is not authorized according the law or the contract;</p> <p>1.2. exceeds limits of authorization;</p> <p>1.3. has no permission from a competent and qualified person, according to law, to use, administer or inspect a computer system or to carry out scientific researches in a computer system;</p>
<p><b>Chapter II – Measures to be taken at the national level</b></p> <p><b>Section 1 – Substantive criminal law</b></p>	
<p><i>Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems</i></p>	
<p><b>Article 2 – Illegal access</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b>Article 9 -Penal acts against confidentiality, integrity and availability of the computer systems data</b></p> <p>1. Illegal access into computer systems is a penal act and its perpetrator shall be liable to imprisonment from six (6) months to three (3) years.</p> <p>2. In case a penal act from paragraph 1 of this Article is committed for the purpose of obtaining computer data its perpetrator shall be liable to imprisonment from six (6) months to four (4) years.</p> <p>3. In case a penal act from paragraph 1 and 2 of this Article is committed by breaching of security measures of computer systems, its perpetrator shall be liable to imprisonment from three (3) to five (5) years.</p>

<p><b>Article 3 – Illegal interception</b>  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b>Article 10 - Unauthorized interception</b>  1. Unauthorized interception of non-public broadcasting of computer information, from, for, to, or within a computer system is a penal act and its perpetrator is liable to imprisonment from six (6) up to three (3) years. If it is committed by a member of a criminal organisation it is liable to imprisonment from one (1) up to five (5) years.  2. Unauthorized interception of electromagnetic emissions from computer systems containing non-public computer data, is a penal act and its perpetrator is liable to imprisonment from one (1) to five (5) years.</p>
<p><b>Article 4 – Data interference</b>  1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.  2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p><b>Article 11 - Unauthorized transfer</b>  1. Modification, deletion, erasure of the computer data or their limitation without authorization is a penal act and its perpetrator is liable to imprisonment from one (1) to three (3) years.  2. Unauthorized data transfer from computer systems is penal act and its perpetrator is liable to imprisonment from three (3) to five (5) years.  3. Unauthorized data transfer from their database through computer systems, is penal act and its perpetrator is liable to imprisonment from three (3) to five (5) years.</p>
<p><b>Article 5 – System interference</b>  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindrance without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</p>	<p><b>Article 12 - Hindrance of computer systems operation</b>  Serious hindrance for the functioning of computer systems, by entering information, transferring, changing, removing or destroying computer data or limiting unauthorized access to such data, is a criminal offence and its perpetrator is liable to imprisonment from three (3) months up to three (3) years. If committed by a member of a criminal</p>

	organisation, its perpetrator is liable to imprisonment from one (1) up to five (5) years.
<p><b>Article 6 – Misuse of devices</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;</p> <p>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p> <p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p>	<p><b>Article 13 - Unauthorized production, possession and attempt</b></p> <p>1. Production, sale, import, distribution or making available in any form, illegally, of any equipment or computer program designed and adapted for the purpose of committing any penal act, shall be liable to imprisonment from one (1) to four (4) years.</p> <p>2. Production, sale, import, distribution or making available in any form, illegally, of the password, access code or other computer information that allow full or partial access to a computer system for the purpose of committing any penal act, shall be liable to imprisonment from one (1) to five (5) years.</p> <p>3. Having in possession, illegally, of equipment, computer program, password, access code or computer information for the purpose of committing any penal act, shall be liable to imprisonment from one (1) to six (6) years.</p> <p>4. The perpetrator, for attempt to commit a penal act from paragraph 2 and 3 of this Article, shall be liable to imprisonment from three (3) months to one (1) year.</p>
<i>Title 2 – Computer-related offences</i>	
<p><b>Article 7 – Computer-related forgery</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p>	<p><b>Article 14 - Computer related penal acts</b></p> <p>1. Unauthorized data entry, change or deletion, of the computer data or unauthorized limitation of access to such a data, resulting in inauthentic data for the purpose of using them for legal purposes, it is penal act and its perpetrator is liable to imprisonment from six (6) months up to three (3) years. If committed by a member of a criminal</p>

	<p>organisation, it is liable to imprisonment from one (1) up to five (5) years.</p> <p>2. For penal act attempt, according to this Article, the perpetrator shall be liable to imprisonment from three (3) months up to one (1) year.</p>
<p><b>Article 8 – Computer-related fraud</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <ul style="list-style-type: none"> <li>a any input, alteration, deletion or suppression of computer data;</li> <li>b any interference with the functioning of a computer system,</li> </ul> <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p><b>Article 15 - Causing loss of asset</b></p> <p>1. Causing a loss in assets to another person by entering information, changing or deleting computer data by means of access limitation to such a data or any other interference into functioning of the computer system with the purpose to ensure economic benefits of his own or to someone else, shall be liable to imprisonment from three (3) to ten (10) years.</p> <p>2. For penal act attempt from paragraph 1 of this Article, the perpetrator shall be liable to imprisonment from three (3) months to one (1) year.</p>
<p><i>Title 3 – Content-related offences</i></p>	
<p><b>Article 9 – Offences related to child pornography</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <ul style="list-style-type: none"> <li>a producing child pornography for the purpose of its distribution through a computer system;</li> <li>b offering or making available child pornography through a computer system;</li> <li>c distributing or transmitting child pornography through a computer system;</li> <li>d procuring child pornography through a computer system for oneself or for another person;</li> <li>e possessing child pornography in a computer system or on a computer-data storage medium.</li> </ul> <p>2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:</p> <ul style="list-style-type: none"> <li>a a minor engaged in sexually explicit conduct;</li> <li>b a person appearing to be a minor engaged in sexually explicit conduct;</li> <li>c realistic images representing a minor engaged in sexually explicit conduct.</li> </ul>	<p><b>Article 16 - Child pornography through computer systems</b></p> <p>1. The person, committing a penal act as foreseen in sub-paragraphs from 1.1 to 1.5. of this paragraph, the perpetrator shall be liable to imprisonment from six (6) months up to three (3) years. If classified that the act was committed in aggravating circumstances, the perpetrator shall be sentenced from one (1) up to ten (10) years.</p> <ul style="list-style-type: none"> <li>1.1. production of child pornography, intended for distribution through a computer system.</li> <li>1.2. provision or making available child pornography through a computer system;</li> <li>1.3. child pornography distribution or broadcast through a computer system;</li> </ul>

<p>3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.</p> <p>4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.</p>	<p>1.4.child pornography procurement through a computer system for itself or others; 1.5. possession of child pornography through a computer system or memory devices of computer data.</p> <p>2. The perpetrator of attempt to commit a penal act from paragraph 1 of this Article, shall be liable to imprisonment from six (6) months to three (3) years.</p>
<p><i>Title 4 – Offences related to infringements of copyright and related rights</i></p>	
<p><b>Article 10 – Offences related to infringements of copyright and related rights</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.</p>	<p><b><u>Law No.2004/45</u></b> <b><u>ON COPYRIGHT AND RELATED RIGHTS</u></b></p> <p>Article 200. Unauthorized use of a Copyright work or subject matter of related rights</p> <p>200.1. Whoever uses without authorization a Copyright work or subject matter of related rights, shall be punished for a criminal offence by imprisonment for up to three years.</p> <p>200.2. If, by the act described in paragraph (1) of this Article, the perpetrator obtained for himself or for another person from 10.000 € to 50.000 €, he or she shall be punished by imprisonment for not less than three months to five years.</p> <p>200.3. If, by the act described in paragraph (1) of this Article, the perpetrator obtained for himself or for another person more than 50.000 €, he or she shall be punished for a criminal offence by imprisonment for not less than six months to eight years.</p>
<p><i>Title 5 – Ancillary liability and sanctions</i></p>	
<p><b>Article 11 – Attempt and aiding or abetting</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present</p>	<p>Law on Prevention and Fight of the Cyber Crime</p>



<p>Convention with intent that such offence be committed.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	
<p><b>Article 12 – Corporate liability</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:</p> <ul style="list-style-type: none"> <li>a a power of representation of the legal person;</li> <li>b an authority to take decisions on behalf of the legal person;</li> <li>c an authority to exercise control within the legal person.</li> </ul> <p>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	<p>Ministry of Justice of Kosovo is in process of amends of the Criminal Procedure Code of Kosovo in order to regulate the liability for criminal offences established in Convention.</p>
<p><b>Article 13 – Sanctions and measures</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.</p> <p>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.</p>	<p>Ministry of Justice of Kosovo is in process of amends of the Criminal Procedure Code of Kosovo in order to adopt legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty</p>
<p><b>Section 2 – Procedural law</b></p>	
<p><b>Article 14 – Scope of procedural provisions</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish the</p>	<p>The procedure is provided by the article 17 of the Law on Prevention and Fight of the Cyber Crime.</p>

powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

- a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
- b other criminal offences committed by means of a computer system; and
- c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

- i is being operated for the benefit of a closed group of users, and
- ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21

**Article 15 – Conditions and safeguards**

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

**Article 16 – Expedited preservation of stored computer data**

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

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige 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 its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

**Article 17 - Prosecution procedure**

1. In urgent and completely justified cases, or reasonable doubt in relation to preparation or committing a penal act through computer systems, for the purpose of collecting evidence and identification of perpetrators, fast saving of computer data or data that refer to traffic data, by becoming subject to a risk to be destroyed or changed, shall be applied procedural provisions as it follows;

1.1. in the course of investigation of a crime, is ordered to store the data by the prosecutor through an order, upon request of an investigation authority, whereas during legal procedure upon courts order.

1.2. the measure that refers to paragraph 1 of this Article is valid for a time period up to ninety (90) days and may be extended for another thirty (30) days.

1.3. prosecutor’s order or judge’s order shall be delivered, immediately to any service provider, or any person who is in possession of data that refer to sub-paragraph 1.1 of this paragraph, pertinent person is obliged to save them quickly in accordance with the terms of confidential preservation.

1.4. in case when data refer to traffic data that are in possession of several service providers, the service provider referring to sub-paragraph 1.3 of this paragraph shall be obliged to provide immediately to the investigation body the necessary information for identification of other service providers in order of being aware of all elements in the used communication chain.

1.5. the prosecutor is obliged that by the end of the investigations notifies in written the persons who are under investigation for a

	crime and information of which are stored.
<p><b>Article 17 – Expedited preservation and partial disclosure of traffic data</b></p> <p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <p>a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and</p> <p>b ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Article 17 - Prosecution procedure</b></p> <p>1. In urgent and completely justified cases, or reasonable doubt in relation to preparation or committing a penal act through computer systems, for the purpose of collecting evidence and identification of perpetrators, fast saving of computer data or data that refer to traffic data, by becoming subject to a risk to be destroyed or changed, shall be applied procedural provisions as it follows;</p> <p>1.1. in the course of investigation of a crime, is ordered to store the data by the prosecutor through an order, upon request of an investigation authority, whereas during legal procedure upon courts order.</p> <p>1.2. the measure that refers to paragraph 1 of this Article is valid for a time period up to ninety (90) days and may be extended for another thirty (30) days.</p> <p>1.3. prosecutor’s order or judge’s order shall be delivered, immediately to any service provider, or any person who is in possession of data that refer to sub-paragraph 1.1 of this paragraph, pertinent person is obliged to save them quickly in accordance with the terms of confidential preservation.</p> <p>1.4. in case when data refer to traffic data that are in possession of several service providers, the service provider referring to sub-paragraph 1.3 of this paragraph shall be obliged to provide immediately to the investigation body the necessary information for identification of other service providers in order of being aware of all elements in the used communication chain.</p> <p>1.5. the prosecutor is obliged that by the end</p>

	<p>of the investigations notifies in written the persons who are under investigation for a crime and information of which are stored.</p>
<p><b>Article 18 – Production order</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>a 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</p> <p>b 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.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the purpose of this article, the term “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:</p> <p>a the type of communication service used, the technical provisions taken thereto and the period of service;</p> <p>b 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;</p> <p>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.</p>	<p>The procedure is provided by the article 18 of the Law on Prevention and Fight of the Cyber Crime</p>
<p><b>Article 19 – Search and seizure of stored computer data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <p>a a computer system or part of it and computer data stored therein; and</p> <p>b a computer-data storage medium in which computer data may be stored in its territory.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, 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, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or</p>	<p><b>Article 18 - Sequestration, copying and maintenance of data</b></p> <p>1. For the purpose of Article 17, sub-paragraph 1.2. the prosecutor shall propose confiscation of objects, equipment containing computer data, information on traffic data, data on the user, from the person or service provider owning them, for the purpose to create copies that might serve as evidence.</p> <p>2. In case objects, equipment containing data that refer to data of justice authorities in order to create copies, under paragraph 1 of this Article, court’s order on forceful confiscation shall be communicated to the prosecutor, who will take measures to fulfil it.</p>

<p>2. These measures shall include the power to:</p> <ul style="list-style-type: none"> <li>a seize or similarly secure a computer system or part of it or a computer-data storage medium;</li> <li>b make and retain a copy of those computer data;</li> <li>c maintain the integrity of the relevant stored computer data;</li> <li>d render inaccessible or remove those computer data in the accessed computer system.</li> </ul> <p>4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to 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 paragraphs 1 and 2.</p> <p>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>3. Copies according to paragraph 1 of this Article are created through technical means, computer programs and procedures which ensure information integrity and security.</p> <p>4. The prosecutor may at any time order search for the purpose of disclosure or collection of necessary evidence about computer system investigation or computer equipment for data storage.</p> <p>5. In case the crime investigation body or the court considers that confiscation of object containing data that refer to paragraph 1 will have a great impact on the activities carried out by the persons who possess such objects, could order creation of copies that would serve as evidence and which are created in compliance with paragraph 3 of this Article.</p> <p>6. In case during an investigation of a computer system or computer equipment for data storage is learned that the required computer data are included into another computer system or other computer data storage device and to which access is provided from the primary system or device, it could be ordered carrying out and search in order to investigate entire computer systems or computer device for the storage of demanded data.</p>
<p><b>Article 20 – Real-time collection of traffic data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <ul style="list-style-type: none"> <li>a collect or record through the application of technical means on the territory of that Party, and</li> <li>b compel a service provider, within its existing technical capability: <ul style="list-style-type: none"> <li>i to collect or record through the application of technical means on the territory of that Party; or</li> <li>ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.</li> </ul> </li> </ul>	<p>Kosovo is not part of the Council of Europe Convention</p>

<p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	
<p><b>Article 21 – Interception of content data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:</p> <p>a collect or record through the application of technical means on the territory of that Party, and</p> <p>b compel a service provider, within its existing technical capability:</p> <p>    i to collect or record through the application of technical means on the territory of that Party, or</p> <p>    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.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Article 19 - Access, obtaining or record of communications</b></p> <p>1. Access to a computer system as well as interception or record of communication carried out by the equipment of the computer systems shall be performed when useful to find the truth as well as facts or identification of perpetrators and could not be achieved based on other evidence.</p> <p>2. The measures that refer to paragraph 1 of this Article shall be carried out upon a proposal of the prosecutor by crime investigation bodies with the assistance of specialized persons which are obliged to maintain confidentiality of the operation carried out.</p> <p>3. The authorization referring to paragraph 2 of this Article shall be given for thirty (30) days, on grounded reasons might be extended for another thirty (30) days, whereas the maximum duration should not exceed a period of four (4) months.</p> <p>4. The prosecutor is obliged that by the end of investigation to inform or write the persons against whom have been undertaken measures as referred to in paragraph 1 of this Article.</p>
<p><b>Section 3 – Jurisdiction</b></p>	
<p><b>Article 22 – Jurisdiction</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:</p>	<p><b><i>Criminal Code of Kosovo</i></b></p>

<p>a in its territory; or</p> <p>b on board a ship flying the flag of that Party; or</p> <p>c on board an aircraft registered under the laws of that Party; or</p> <p>d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.</p> <p>2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.</p> <p>3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.</p> <p>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.</p>	
<p><b>Chapter III – International co-operation</b></p>	
<p><b>Article 24 – Extradition</b></p> <p>1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.</p> <p>b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.</p> <p>2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.</p> <p>3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.</p> <p>4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the</p>	<p>Kosovo is not part of the Council of Europe Convention on Extradition. However the Criminal Procedure Code provides with provisions regarding the Extradition procedure</p>



criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure

**Article 25 – General principles relating to mutual assistance**

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in

**Article 20 - International Cooperation**

1. Kosovar authorities shall cooperate directly according to provisions of the law, by respecting obligations deriving from international legal instruments, with counterpart institutions of other states as well as international organizations specialised in this field.

2. Cooperation according to paragraph 1 of this Article could consist, in international legal assistance in penal issues, extradition, identification, block, confiscation of products and means used in carrying out the penal act, carrying out investigations, exchange of information, technical assistance or information collection, specialized training of personnel as well as other activities.

**Article 21 - Investigations**

<p>Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.</p> <p>5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.</p>	<p>1. States and other organizations, upon their request could carry out investigation in cooperation with Kosovar authorities to prevent and fight cyber crime in the entire territory of Kosovo.</p> <p>2. General investigations that refer to paragraph 1 of this Article are carried out on basis of bilateral and multilateral agreements.</p> <p>3. The representatives of the competent Kosovar authorities may undertake investigations to be carried out in the territory of other countries in compliance with provisions of international agreements.</p>
<p><b>Article 26 – Spontaneous information</b></p> <p>1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.</p> <p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	<p><b>Article 26 - Legal provisions for providing information and data, necessary for the foreign authorities</b></p> <p>The Kosovar competent authorities may deliver under their official duty to foreign competent authorities, by respecting legal provisions concerning protection of personal information, information and data, required by foreign competent authorities to disclose committed acts through computer system or to solve issues related to these crimes.</p>
<p><b>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</b></p> <p>1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.</p> <p>b The central authorities shall communicate directly with each other;</p> <p>c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the</p>	<p>Kosovo currently has no mutual agreement with countries. In absence of such Agreements Kosovo provide legal assistance to foreign countries based on Principle of Reciprocity.</p>

names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

<p>e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.</p>	
<p><b>Article 28 – Confidentiality and limitation on use</b></p> <p>1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:</p> <p>a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or</p> <p>b not used for investigations or proceedings other than those stated in the request.</p> <p>3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.</p> <p>4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.</p>	<p>Article 20 of the Law on Prevention and Fight of the Cyber Crime.</p>
<p><b>Article 29 – Expedited preservation of stored computer data</b></p> <p>1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.</p> <p>2 A request for preservation made under paragraph 1 shall specify:</p> <p>a the authority seeking the preservation;</p> <p>b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;</p> <p>c the stored computer data to be preserved and its relationship to the offence;</p> <p>d any available information identifying the custodian of the stored computer data or the location of the computer system;</p> <p>e the necessity of the preservation; and</p> <p>f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.</p> <p>3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the</p>	<p><b>Article 23 - Requirements for accelerated data maintenance</b></p> <p>1. Within the international cooperation, foreign competent authorities might request through the contact point to store quickly computer data or data concerning the traffic data that do exist inside a computer system in the territory of Kosovo, in relation to which a foreign authority have made a request for international legal assistance in penal issues.</p> <p>2. The request for rapid storage according to paragraph 1 shall include the following information:</p> <p>2.1. authority who requests the storage;</p> <p>2.2. a brief presentation of facts that are subject to a crime investigation and the legal ground;</p> <p>2.3. computer data requested to be stored;</p>

<p>purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.</p> <p>4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.</p> <p>5 In addition, a request for preservation may only be refused if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p> <p>6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.</p> <p>4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.</p>	<p>2.4. any information available, required to identify the computer data owner and the location of the computer system;</p> <p>2.5. service of the computer system and the need to store them;</p> <p>2.6. the purpose of the foreign authority for formulation of a request on international legal assistance in penal matters;</p> <p>3. The storage request is executed according to Article 17 for a sixty (60) days period. This storage is valid until a decision is taken by competent Kosovar authorities, in relation to the request on international legal assistance in penal matters.</p>
<p><b>Article 30 – Expedited disclosure of preserved traffic data</b></p> <p>1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.</p> <p>2 Disclosure of traffic data under paragraph 1 may only be withheld if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	<p><b>Article 24 - Data storage</b></p> <p>If, in the execution of the request formulated according to Article 23, paragraph 1 of this law, a service provider in a foreign country is found out that it is in possession of the data concerning to traffic data, the service of fight against cyber crime will inform immediately the requesting foreign authority about this, by communicating also all information for identification of the pertinent service provider.</p>
<p><b>Article 31 – Mutual assistance regarding accessing of stored computer data</b></p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p>	<p>The procedure is provided by the article 20 of the Law on Prevention and Fight of the Cyber Crime</p>

<p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <p>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</p> <p>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</p>	
<p><b>Article 32 – Trans-border access to stored computer data with consent or where publicly available</b></p> <p>A Party may, without the authorisation of another Party:</p> <p>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</p> <p>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</p>	<p><b>Article 25 - Access to public, open sources</b></p> <p>1. Foreign competent authority may have access and can accept, through the system located in its territory, computer data stored in Kosovo, if it has the approval of the authorized person, according to legal provisions, to make available through the computer system, without filing request to the Kosovar authorities.</p> <p>2. Foreign competent authority may have access to public, open Kosovar sources of computer data, without needing to file request to the Kosovar authorities.</p>
<p><b>Article 33 – Mutual assistance in the real-time collection of traffic data</b></p> <p>1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.</p>	<p>The procedure is provided by the article 18 of the Law on Prevention and Fight of the Cyber Crime</p>
<p><b>Article 34 – Mutual assistance regarding the interception of content data</b></p> <p>The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.</p>	<p>The procedure is provided by the article 18 of the Law on Prevention and Fight of the Cyber Crime</p>
<p><b>Article 35 – 24/7 Network</b></p> <p>1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its</p>	<p><b>Article 22 - Contact point</b></p> <p>1. In order to ensure a permanent international cooperation in the field of cyber crime, the Government shall make available a permanent contact point.</p>

<p>domestic law and practice, directly carrying out the following measures:</p> <ul style="list-style-type: none"> <li>a the provision of technical advice;</li> <li>b the preservation of data pursuant to Articles 29 and 30;</li> <li>c the collection of evidence, the provision of legal information, and locating of suspects.</li> </ul> <p>2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.</p> <p>b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	<p>2. This permanent contact point possesses the following competencies:</p> <ul style="list-style-type: none"> <li>2.1. provides specialized assistance and information on the legislation in the scope of cyber crime as well as informs contact points of other states;</li> <li>2.2. orders rapid data storage as well as confiscation of equipment containing computer data or data concerning traffic data demanded by a foreign competent authority;</li> <li>2.3. executes or assists in execution, according to legal provisions, in cases of cyber crime fight, by cooperating with the entire Kosovar competent authorities.</li> </ul> <p>3. Government in a period of six (6) months from the entry into force of this law with a subsidiary act stipulates the establishment of point of contact stipulated in paragraph 1 of this Article.</p>
<p><b>Article 42 – Reservations</b></p> <p>By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.</p>	