www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Version July 2016

Cybercrime legislation – country profile

[Kosovo*[1]]

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
www.coe.int/cybercrime

Country:	**Republic of Kosovo**
Signature of Convention:	
Ratification/accession:	

[1] This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

Provisions of the Convention	
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data*":* 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	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 3 - Definitions** 1. Terms used in this law have the following meaning: 1.1. **Cyber crime -** 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.**Computer system -** 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. **Automatic data processing -** a process by which the data are processed to the computer system through computer programs; 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 which, although it does not present a real person, simulates, in such credible way a minor with explicit sexual behaviour. 1.11. **Interception -** obtaining, illegal seizure of the data from unauthorized persons. **Article 4 - Unauthorized actions** 1. Pursuant to this Law, a person acts are considered unauthorized actions, if the person: 1.1. is not authorized according the law or the contract; 1.2. exceeds limits of authorization; 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;
Chapter II – Measures to be taken at the national level ***Section 1 – Substantive criminal law***	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access 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.	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 9 -Penal acts against confidentiality, integrity and availability of the computer systems data** 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. 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. 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.

Article 3 – Illegal interception 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.	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 10 - Unauthorized interception** 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.
Article 4 – Data interference 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.	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 11 - Unauthorized transfer** 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.
Article 5 – System interference 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 hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 12 - Hindrance of computer systems operation** 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 organisation, its perpetrator is liable to imprisonment from one (1) up to five (5) years.
Article 6 – Misuse of devices	

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: a the production, sale, procurement for use, import, distribution or otherwise making available of: 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; 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 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. 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. 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.	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 13 - Unauthorized production, possession and attempt** 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. 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. 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. 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.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery 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	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 14 - Computer related penal acts** 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

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.	is liable to imprisonment from six (6) months up to three (3) years. If committed by a member of a criminal organisation, it is liable to imprisonment from one (1) up to five (5) years. 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.
Article 8 – Computer-related fraud 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: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 15 - Causing loss of asset** 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. 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.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 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: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 16 - Child pornography through computer systems** 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. 1.1. production of child pornography, intended for distribution through a computer system. 1.2. provision or making available child pornography through a computer system; 1.3. child pornography distribution or broadcast through a computer system; 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

a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 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. 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.	devices of computer data. 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.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 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. 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. 3 A Party may reserve the right not to impose criminal liability under	**CODE NO. 04/L-082** **CRIMINAL CODE OF THE REPUBLIC OF KOSOVO** **Article 296** **Violation of copyrights** 1. Whoever, under his own name, or somebody else's name discloses or otherwise communicates to the public a copyrighted work or a performance of another, in whole or in part, shall be punished by a fine and imprisonment of three (3) months to up to three (3) years. 2. Whoever during use of copyrighted work or a performance of another intentionally fails to state the name, pseudonym or mark of the author or performer, when this is required by law, shall be punished by fine and imprisonment for up to one (1) year. 3. Whoever distorts, mutilates or otherwise harms a copyrighted work or a performance of another, and discloses it in such form or otherwise communicates it in such form to the public shall be punished for by fine or imprisonment for up to one (1) year. 4. Whoever performs or otherwise communicates to the public a copyrighted work or a performance of another in an indecent manner, which is prejudicial to the honor and reputation of the author or performer, shall be punished by a fine or imprisonment for up to one (1) year.

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.	5. Whoever without authorization uses a copyrighted work or subject matter of related rights, shall be punished by imprisonment up to three (3) years. 6. If, during the commission of the offense described in paragraph 5 of this Article, the perpetrator obtained for himself or for another person at least ten thousand (10,000) EUR but less than fifty thousand (50,000) EUR, he or she shall be punished by a fine and imprisonment of not less than three (3) months to five (5) years. 7. When the perpetrator of the offense in paragraph 5 of this Article obtains for himself, herself, or for another person more than fifty thousand (50,000) EUR, he or she shall be punished by a fine and imprisonment of not less than six (6) months to eight (8) years. 8. The objects and the equipment for their manufacturing provided for in this Article shall be confiscated.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 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 Convention with intent that such offence be committed. 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. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Criminal Code of the Republic of Kosovo** **Article 33** **Assistance** 1. Whoever intentionally assists another person in the commission of a criminal offense shall be punished more leniently. 2. Assistance in committing a criminal offense includes, but is not limited to: giving advice or instruction on how to commit a criminal offense; making available the means to commit a criminal offense; creating conditions or removing the impediments to the commission of a criminal offense; or, promising in advance to conceal evidence of the commission of a criminal offense, the perpetrator or identity of the perpetrator, the means used for the commission of a criminal offense, or the profits or gains which result from the commission of a criminal offense. **Article 28** **Attempt** **1.** Whoever intentionally takes action toward the commission of an offense but the action is not completed or the elements of the intended offense are not fulfilled has attempted to commit a criminal offense.

	2. An attempt to commit a criminal offense for which a punishment of three or more years may be imposed shall be punishable. An attempt to commit any other criminal offense shall be punishable only if expressly provided for by law. 3. A person who attempts to commit a criminal offense shall be punished as if he or she committed the criminal offense, however, the punishment may be reduced.
Article 12 – Corporate liability 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: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 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. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Criminal Code of Kosovo of the Republic of Kosovo** **Article 40** **Criminal liability of legal persons** 1. A legal person is liable for the criminal offence of the responsible person, who has committed a criminal offence, acting on behalf of the legal person within his or her authorizations, with the purpose to gain a benefit or has caused damages for that legal person. The liability of legal person exists even when the actions of the legal person were in contradiction with the business policies or the orders of the legal person. 2. Under the conditions provided for in paragraph 1 of this Article, the legal person shall also be liable for criminal offences in cases of the responsible person, who has committed the criminal offence, who was not sentenced for that criminal offence. 3. The liability of the legal person is based on the culpability of the responsible person. 4. The subjective element of the criminal offence, which exists only for the responsible person, shall be evaluated in relation with the legal person, if the basis for the liability provided for in paragraph 1 of this Article, was fulfilled. **Article 119** **Special provisions for legal persons** The criminal offenses for which a legal person may be criminally liable, the criminal liability of a legal person, the criminal sanctions which may be applied to a legal person and special provisions governing criminal procedures applicable to a legal person shall be provided for by this Code or separate law.
Article 13 – Sanctions and measures 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. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 9 -Penal acts against confidentiality, integrity and availability of the computer systems data** 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.

criminal or non-criminal sanctions or measures, including monetary sanctions.	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. 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. **Criminal Code of Kosovo of the Republic of Kosovo** **Article 202** **Infringing privacy in correspondence and computer databases** 1. Whoever, without authorization, opens a letter, telegram, facsimile or some other sealed document, package or electronic communication of another person or in any other way violates the privacy of such materials or, without authorization, withholds, conceals, destroys or delivers to another person a letter, telegram, facsimile, electronic communication or some other sealed document or package of another person shall be punished by a fine and by imprisonment of up to six (6) months. 2. Whoever, without authorization, intrudes upon the computer database of another person or uses data obtained from such database or makes such data available to another person shall be punished by a fine and by imprisonment of up to one (1) year. 3. When the offense provided for in paragraph 1 or 2 of this Article is committed for the purpose of obtaining a material benefit for himself or herself or another person or of causing damage to another person, the perpetrator shall be punished by a fine and imprisonment of up to three (3) years. 4. When the offense provided for in paragraph 1, or 2 or 3 of this Article is committed by an official person, in abusing his or her position or authorizations, the perpetrator shall be punished by imprisonment of three (3) months to three (3) years, in the case of the offense provided for in paragraph 1 or 2 of this Article or by imprisonment of one (1) to five (5) years, in the case of the offense provided for in paragraph 3 of this Article. **Article 339** **Intrusion into computer systems** 1. Whoever, without authorization and with the intent to obtain an unlawful material benefit for himself, herself or another person or to cause damage to another person, alters, publishes, deletes, suppresses or destroys computer data or programs or in any other way intrudes into a computer system shall be punished by a fine and imprisonment of up to three (3) years.

	2. When the offense provided for in paragraph 1 of this Article results in a material benefit exceeding tent thousand (10,000) EUR, or material damage exceeding ten thousand (10,000) EUR, the perpetrator shall be punished by a fine and imprisonment of six (6) months to five (5) years. **Article 33** **Assistance** 1. Whoever intentionally assists another person in the commission of a criminal offense shall be punished more leniently. 2. Assistance in committing a criminal offense includes, but is not limited to: giving advice or instruction on how to commit a criminal offense; making available the means to commit a criminal offense; creating conditions or removing the impediments to the commission of a criminal offense; or, promising in advance to conceal evidence of the commission of a criminal offense, the perpetrator or identity of the perpetrator, the means used for the commission of a criminal offense, or the profits or gains which result from the commission of a criminal offense.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the 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.	**Criminal Code of Kosovo of the Republic of Kosovo** This is regulated by Criminal Procedure Code. Concretely, articles as below regulate the procedure of investigation which is applicable for all criminal offences, including criminal offences related to computer system: CHAPTER IX INITIATION OF INVESTIGATIONS AND CRIMINAL PROCEEDINGS 1. STAGES OF THE CRIMINAL PROCEEDING - Article 68 <u>Stages of a Criminal Proceeding</u> A criminal proceeding under this Criminal Procedure Code shall have four distinct stages: the investigation stage, the indictment and plea stage, the main trial stage and the legal remedy stage. A criminal proceeding may be preceded by initial steps by the police or information gathering under Article 84 of this Code. - Article 68 to 71, - Article 81 to 95,

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 101 to 104. - Article 17 of the Law on Cybercrime Fight and Prevention regulates Prosecution Procedure.
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.	Constitution of the Republic of Kosovo Article 22 [Direct Applicability of International Agreements and Instruments] Human rights and fundamental freedoms guaranteed by the following international agreements and instruments are guaranteed by this Constitution, are directly applicable in the Republic of Kosovo and, in the case of conflict, have priority over provisions of laws and other acts of public institutions: (1) Universal Declaration of Human Rights; (2) European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols; (3) International Covenant on Civil and Political Rights and its Protocols; (4) Council of Europe Framework Convention for the Protection of National Minorities; (5) Convention on the Elimination of All Forms of Racial Discrimination; (6) Convention on the Elimination of All Forms of Discrimination Against Women; (7) Convention on the Rights of the Child; (8) Convention against Torture and Other Cruel, Inhumane or Degrading Treatment or Punishment;
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be	**Article 17 - Prosecution procedure**

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.	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.
Article 17 – Expedited preservation and partial disclosure of traffic data 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: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **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

transmission of that communication; and 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	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.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: 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 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 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: a the type of communication service used, the technical provisions	**LAW No. 04/L-109 ON ELECTRONIC COMMUNICATIONS** Article 68 Personal Data Preservation and Administration for the criminal proceedings purposes: 1. Regardless of other definitions in this Law, the entrepreneurs of public electronic communications services and networks shall be obliged to store and administrate, for a period not longer than one (1) year, the data files of their subscribers referred to in paragraph 2 of this Article. Such storage shall be paid for by state funds in accordance with the procedure established by the Government. 2. Entrepreneurs providing electronic communications networks and/or services shall ensure that the following categories of data are retained: 2.1. data necessary to trace and identify the resource of a communication

taken thereto and the period of service; 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; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	concerning fixed network telephony and mobile telephony: 2.1.1. the calling telephone number; 2.1.2. the name and address of the subscriber or registered user; 2.2. concerning Internet access, Internet e-mail and Internet telephony: 2.2.1. the user ID (s) allocated; 2.2.2. the user ID and telephone number allocated to any communication entering the public telephone network; 2.2.3. 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; 2.3. data necessary to identify the destination of a communication concerning fixed network telephony and mobile telephony: 2.3.1. the number(s) dialed (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; 2.3.2. the name(s) and address(es) of the subscriber(s) or registered user(s); 2.4. concerning Internet e-mail and Internet telephony: 2.4.1. the user ID or telephone number of the intended recipient(s) of an Internet telephony call; 2.4.2. the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication; 2.5. data necessary to identify the date, time and duration of a communication: 2.5.1. concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication; 2.6. concerning Internet access, Internet e-mail and Internet telephony: 2.6.1. 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; 2.6.2. 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;

	2.7. data necessary to identify the type of communication: 2.7.1. concerning fixed network telephony and mobile telephony: the telephone service used; 2.7.2. concerning Internet e-mail and Internet telephony: the Internet service used; 2.8. data necessary to identify users' communication equipment or what purports to be their equipment: 2.9. concerning fixed network telephony, the calling and called telephone numbers; 2.10. concerning mobile telephony; 2.11. the calling and called telephone numbers; 2.12. the International Mobile Subscriber Identity (IMSI) of the calling party; 2.13. the International Mobile Equipment Identity (IMEI) of the calling party; 2.14. the IMSI of the called party; 2.15. the IMEI of the called party; 2.16. 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; 2.17. concerning Internet access, Internet e-mail and Internet telephony: 2.18. the calling telephone number for dial-up access; 2.19. the digital subscriber line (DSL) or other end point of the originator of the communication; 2.20. data necessary to identify the location of mobile communication equipment: 2.20.1. the location label (Cell ID) at the start of the communication; 2.21. 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. Data, listed in paragraph 2 of this Article shall be made available, in the electronic format as well, to the authorities prescribed in the legislation of Criminal Procedure in force, upon their request.

	CHAPTER XVII **SUPERVISION AND MONITORING OF ELECTRONIC COMMUNICATIONS TRAFFIC** **Article 104** **Supervision and Monitoring** 1.Entrepreneurs providing electronic communications networks and/or services shall have the right to record and store technical data on electronic communications and their participants only to the extent that is necessary to ensure economic activities of the said entrepreneurs. Entrepreneurs providing electronic communications networks and/or services must submit, in accordance with the procedure established by the law, to operational investigation services, pretrial investigation institutions, prosecutors, courts or judges information which is available to them and which is necessary to prevent, investigate and detect criminal acts. Such information shall be submitted, immediately and free of charge, by entrepreneurs providing electronic communications networks and/or services to the main institutions of operational investigation services and pre-trial investigation institutions designated by the Government in electronic form in response to their enquiries. Pre-trial investigation institutions designated by the Government shall provide their subdivisions and/or other pre-trial investigation institutions with access to such information in accordance with the procedure established by the Government. All persons taking part in the exchange of information shall make necessary arrangements to ensure data security in accordance with the procedure and conditions set forth by the Government; the additional equipment necessary for this purpose shall be obtained from and maintained by Government funds. If the information presented by an entrepreneur providing electronic communications networks and/or services needs to be confirmed for a pre-trial investigation purposes, the pre-trial investigation officer shall directly address the entrepreneur in writing and the entrepreneur shall provide a written response. 2. Entrepreneurs providing electronic communications networks and/or services shall store technical information used during the transmission of electronic communications traffic only for a period that is necessary to ensure their

	economic activity which will not exceed six months, except for cases referred to in Article 68 of this Law; where such information is necessary for operational investigation services, pre-trial investigation institutions, prosecutors, courts or judges to prevent, investigate and detect criminal acts, entrepreneurs providing electronic communications networks and/or services shall, on instruction from an institution (operational investigation service) authorized by the Government, store such information for a longer period, but no longer than additional six (6) months. Such storage shall be paid for by state funds in accordance with the procedure established by the Government. 3. Where there is a reasoned court ruling, entrepreneurs providing electronic communications networks and/or services must provide operational investigation services, in accordance with the procedure established by the law, and pre-trial investigation institutions, in accordance with the procedure established by the Legislation of Criminal Procedure in force, with technical possibilities to exercise control over the content of information transmitted by electronic communications networks. Equipment necessary for this purpose shall be obtained from and maintained by Kosovo budget. 4. A Government authorized institution (operational investigation service) shall organize and provide, in accordance with the procedure established by the Government, each operational investigation service and, in the event of criminal proceedings, each pre-trial investigation institution with a technical opportunity to exercise independent control over the content of information transmitted by electronic communications networks. 5. Entrepreneurs providing electronic communications networks and/or services shall inform a Government authorized institution (operational investigation service) and the Authority about any changes to be made in their networks or at points of interconnection with other electronic communications operators, which may affect the operation of equipment referred to in paragraphs 1 and/or 3 of this Article and the volume of information presented, as soon as they get to know about it.

	6. Technical commands sent by an electronic communications network to start or discontinue wire tapping or any other control of the information transmitted over electronic communications networks shall be safe kept at the premises of a Government authorized institution (operational investigation service) in such a way that would prevent the command data to be modified by the Government authorized institution which has sent such commands or by the entrepreneur which has received them. The Prosecutor General or his authorized prosecutor shall exercise control over compliance with the provisions of this paragraph.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 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. 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 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system.	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 18 - Sequestration, copying and maintenance of data** 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. 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 fulfill it. 3. Copies according to paragraph 1 of this Article are created through technical means, computer programs and procedures which ensure information integrity and security. 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. 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

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. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	compliance with paragraph 3 of this Article. 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.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 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. 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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Articles 18 and 19 of the Law on Cybercrime Fight and Prevention regulates this issue. Also, articles 67 (Subscribers Registration), 68 (Personal Data Preservation and Administration for the criminal proceedings purposes) and 104 (Supervision and Monitoring) of the Law on Electronic Communication also are relevant to the above mentioned point.

Article 21 – Interception of content data 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: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 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. 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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 19 - Access, obtaining or record of communications** 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. 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. 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. 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.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 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: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed	Criminal Code of Kosovo of the Republic of Kosovo **Article 116** **Applicability of criminal laws of the Republic of Kosovo to foreign person committing criminal offenses** **outside the territory of the Republic of Kosovo** 1. The criminal laws of the Republic of Kosovo apply to any person who is a foreign person if: 1.1. such person has committed a criminal offense outside the territory of the Republic of Kosovo against a national of the Republic of Kosovo even when such

outside the territorial jurisdiction of any State. 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. 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. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 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.	a criminal offense is not referred to in Article 115 of this Code; 1.2. this act is also punishable at the place of its commission; and 1.3. the perpetrator is found on the territory of the Republic of Kosovo or has been transferred to the Republic of Kosovo. **Article 117** **Special prerequisites for prosecution of criminal offenses committed outside the territory of the Republic of Kosovo** 1. In the cases provided for in Article 114 of this Code, if criminal proceedings have commenced but have not been completed in another jurisdiction, criminal proceedings shall be initiated in the Republic of Kosovo only upon the authorization of the Chief State Prosecutor of the Republic of Kosovo. 2. In the cases provided for in Articles 115 and 116 of this Code, criminal proceedings shall not be initiated if: 2.1. the perpetrator has completely served the punishment imposed in another jurisdiction; 2.2. the perpetrator has been acquitted in another jurisdiction by a final court judgment or the punishment was waived or prescribed by statutory limitation; or 2.3. criminal proceedings for that criminal offense in another jurisdiction may only be initiated upon request of the injured party and such request has not been presented. 3. Criminal proceedings pursuant to Article 118 of this Code may be initiated in the Republic of Kosovo only upon the authorization of the Chief State Prosecutor of the Republic of Kosovo. 4. In the cases provided for in Article 114 of this Code the criminal prosecution of a foreign person may be transferred to a foreign jurisdiction on the condition of reciprocity.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this	**LAW NO. 04/L-213 ON INTERNATIONAL LEGAL COOPERATION IN CRIMINAL MATTERS**

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. 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. 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. 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. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the 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	**CHAPTER II** **EXTRADITION** **SUB CHAPTER I** **EXTRADITION FROM THE REPUBLIC OF KOSOVO TO OTHER STATES** **Article 6** **Purpose** 1. A person sought by another state for the purpose of criminal proceedings or for the enforcement of a sentence may be extradited from the Republic of Kosovo to that state under the conditions foreseen by the present law. 2. The following persons cannot be extradited against their will: 2.1. Kosovo citizens, unless otherwise provided by an international agreement between the Republic of Kosovo and the requesting state or by international law, as per Article 35 paragraph 4. of the Constitution of the Republic of Kosovo. An international agreement may be concluded for the purpose of extraditing an individual; 2.2. persons who have been granted political asylum in the Republic of Kosovo; 2.3. foreigners who enjoy immunity of jurisdiction in the Republic of Kosovo, within the limits of international obligations assumed by the Republic of Kosovo. 3. The status of a citizen of the Republic of Kosovo or of a political refugee is determined at the time of receipt of the request for extradition. **Article 8** **Place of perpetration** 1. Extradition shall not be permitted for criminal offences fully committed in the territory of the Republic of Kosovo and may not be permitted for criminal offences partially committed in the territory of the Republic of Kosovo. 2. If a criminal offence has been committed against a citizen of the Republic of Kosovo outside the territory of the Republic of Kosovo, extradition may be permitted on condition that national judicial authorities do not commence or terminate criminal proceedings for the same offence. **Article 9** **Double criminality** Extradition shall be permitted only for criminal offences punishable by both the national law and by the law of the requesting state. **Article 10** **Criminal offences for which extradition is permitted** 1. When extradition is requested for criminal prosecution, it shall be permitted

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	only for criminal offences where the maximum period punishable by deprivation of liberty is at least one (1) year or by a more severe punishment under both the national law and the law of the requesting state. 2. When extradition is requested for the enforcement of a sentence, it may be permitted if the duration of the sentence, or the remaining part of the sentence, exceeds the period of four (4) months of imprisonment. 3. If the request for extradition includes several separate offences each of which is punishable under the national law and the law of the requesting state by deprivation of liberty, but some of which do not fulfill the condition with regard to the amount of punishment which may imposed, extradition may be permitted with respect to all of them. **Article 11** **Expiry of statutory limitation period** Extradition shall not be permitted in cases where, pursuant to the national law or the law of the requesting state, the statutory limitation period for criminal prosecution or enforcement of sentence is expired. **Article 12** **Reasonable suspicion** Extradition shall be permitted when there is sufficient evidence to support a reasonable suspicion that the person has committed the criminal offence for which extradition is requested or if there is an enforceable judgment thereof. **Article 13** **Ne bis in idem** 1. Extradition shall not be permitted if a final judgment was passed by a national judicial authority against the person sought for the criminal offence or offences for which extradition is requested. Extradition may be permitted if national judicial authorities have decided not to commence or to terminate proceedings for the same criminal offence. 2. Extradition shall not be permitted if a final judgment was passed by the judicial authorities of a third state against the person sought for the criminal offence for which extradition is requested provided that an international agreement on mutual recognition and enforcement of criminal judgments between the Republic of Kosovo and that third state is in force. **Article 14** **Political offences**

	1. Extradition shall not be permitted if the offence upon which the request is based is a political offence or an offence connected to a political offence. 2. For the purposes of this Law, the following offences shall not be deemed to be political offences: 2.1. murder and attempted murder of the head of state or his or her family members; 2.2. genocide, crimes against humanity, war crimes, and terrorism. **Article 15** **Military offences** Extradition shall not be permitted for criminal offences under military law which are not criminal offences under ordinary criminal law. **Article 16** **Death penalty and lifelong imprisonment** 1. Extradition is not permitted for criminal offences which under the law of the requesting state are punishable by the death penalty, unless the requesting state gives assurances which are considered sufficient that the death penalty will not be imposed or carried out. 2. Extradition may not be permitted if the offence upon which the request is based is, under the law of the requesting State, punishable by life imprisonment or other custodial sanction for life, or if the person sought was sentenced to such a punishment and there is no review of the punishment or sanction either upon request or *proprio motu* after a period of no longer than twenty (20) years. **Article 17** **Non-discrimination clause and human rights standards** 1. Extradition shall not be permitted if there are reasonable grounds to believe that the request for extradition has been made for the purpose of prosecuting or punishing the person because of his/her race, religion, gender, nationality, political opinions, ethnicity, language, disability, sexual orientation, association in any social group, or if the person's position in society may be prejudiced for any of these reasons. 2. Extradition shall not be permitted if there are reasonable grounds to believe that the person sought for extradition may be subjected to torture or to cruel, inhuman, or degrading treatment or punishment.

	3. Extradition shall not be permitted if there are reasons to believe that the person will not be provided with the minimum guarantees for a fair trial as provided for by the Constitution of the Republic of Kosovo, in the requesting state. 4. Extradition sought for the enforcement of a sentence imposed by a judgment rendered in absentia shall be permitted only if the proceedings against the person respected the recognized minimum rights of defence of any person accused of committing a criminal offence. Extradition may also be permitted if the requesting state gives assurances considered sufficient to guarantee that the person sought has the right to a retrial in order to ensure the minimum rights of defence. 5. Extradition shall not be permitted if there are doubts that the person will be or has been tried or punished in the requesting state by an extraordinary or temporary court, unless the requesting state gives assurances considered sufficient to guarantee that the trial or a retrial will be carried out by a regular court in compliance with the law. 6. Extradition shall not be permitted for any other grounded reason which would account for a violation of the international law or other human rights standards.
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	**LAW NO. 04/L-213 ON INTERNATIONAL LEGAL COOPERATION IN CRIMINAL MATTERS** **CHAPTER VI** **MUTUAL LEGAL ASSISTANCE** **Article 80** **Principle** 1. Upon the request of a judicial authority of another state, national judicial authorities shall provide assistance to that state for criminal proceedings conducted for offences whose punishment, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting state. 2. Legal assistance within the meaning of paragraph 1 of this Article shall be any type of support given to foreign authorities regardless of whether the foreign proceedings are conducted by a court or by a prosecution office or if the legal assistance is to be provided by a court or by a prosecution office. 3. Legal assistance under this Chapter may also be provided or requested for the taking of provisional measures for the purpose of preserving evidence,

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 Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 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.	maintaining an existing situation or protecting endangered legal interests, 4. National judicial authorities shall give priority to the execution of requests for mutual legal assistance and take into account any procedural deadlines and any other terms indicated by the requesting state. **Article 81** **Extended mutual legal assistance** Assistance shall also be provided in support of proceedings brought by administrative authorities with regard to acts which are punishable by the national law or by the law of the requesting state for being infringements of laws which could lead to criminal proceedings.
Article 26 – Spontaneous information 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. 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.	**LAW NO. 04/L-213 ON INTERNATIONAL LEGAL COOPERATION IN CRIMINAL MATTERS** **Article 92** **Spontaneous exchange of information** 1. Without hindering the course of investigations or criminal proceedings, national judicial authorities may, without a prior request, transmit to the competent authorities of another state information collected during their investigations if they consider that the disclosure of such information may assist the receiving state in initiating or carrying out investigations or criminal proceedings, or if it may lead to a request for mutual legal assistance by the receiving state. 2. The Ministry may establish conditions for the use of information referred to in the paragraph 1. of this Article. **Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 26 - Legal provisions for providing information and data, necessary for the foreign authorities** 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.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 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. 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. b The central authorities shall communicate directly with each other; 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 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.	**LAW ON INTERNATIONAL LEGAL COOPERATION IN CRIMINAL MATTERS** **CHAPTER I** **GENERAL PROVISIONS** **Article 1** **Purpose** 1. This law establishes the conditions and procedures for international legal cooperation in criminal matters between the Republic of Kosovo and other states, unless otherwise provided by international agreements. 2. International legal cooperation may also take place in relation to international organisations or institutions, as appropriate. 3. In the absence of an international agreement between the Republic of Kosovo and another state, international legal cooperation shall be administered on the basis of the principle of reciprocity. **Article 4** 1. Requests for international legal cooperation shall be transmitted through the Ministry of Justice. Where necessary, diplomatic channels may also be used. 2. In urgent cases, national judicial authorities may provide assistance even if the request is received directly, through INTERPOL, or in any other form which produces a written record, on condition that the requesting state assures that it will send the request in original within thirty (30)days in accordance with paragraph 1. of this Article. 4. The Minister may allow direct cooperation between national and foreign judicial authorities, as deemed appropriate.

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. 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.	
Article 28 – Confidentiality and limitation on use	

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. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 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. 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.	**Article 5** **Confidentiality** 1. The Ministry shall ensure the confidentiality of requests for international legal cooperation and of the information contained in the requests if the requesting state so requires. 2. If the requirement referred to in paragraph 1. of this Article cannot be met, the Ministry shall notify the requesting state thereof.
Article 29 – Expedited preservation of stored computer data 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. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 23 - Requirements for accelerated data maintenance** 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. 2. The request for rapid storage according to paragraph 1 shall include the following information: 2.1. authority who requests the storage; 2.2. a brief presentation of facts that are subject to a crime investigation and the legal ground; 2.3. computer data requested to be stored; 2.4. any information available, required to identify the computer data owner and the location of the computer system; 2.5. service of the computer system and the need to store them;

for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 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 purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 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. 5 In addition, a request for preservation may only be refused 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 the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 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. 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.	2.6. the purpose of the foreign authority for formulation of a request on international legal assistance in penal matters; 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.
Article 30 – Expedited disclosure of preserved traffic data 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	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 24 - Data storage** 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

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. 2 Disclosure of traffic data under paragraph 1 may only be withheld 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 the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	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.
Article 31 – Mutual assistance regarding accessing of stored computer data 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. 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. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**LAW ON INTERNATIONAL LEGAL COOPERATION IN CRIMINAL MATTERS** 1.Requests for international legal cooperation shall be transmitted through the Ministry of Justice. Where necessary, diplomatic channels may also be used. 2. In urgent cases, national judicial authorities may provide assistance even if the request is received directly, through INTERPOL, or in any other form which produces a written record, on condition that the requesting state assures that it will send the request in original within thirty (30)days in accordance with paragraph 1. of this Article. **Article 80** **Paragraph 4** 4. National judicial authorities shall give priority to the execution of requests for mutual legal assistance and take into account any procedural deadlines and any other terms indicated by the requesting state. **Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 23 - Requirements for accelerated data maintenance** 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. 2. The request for rapid storage according to paragraph 1 shall include the following information:

	2.1. authority who requests the storage; 2.2. a brief presentation of facts that are subject to a crime investigation and the legal ground; 2.3. computer data requested to be stored; 2.4. any information available, required to identify the computer data owner and the location of the computer system; 2.5. service of the computer system and the need to store them; 2.6. the purpose of the foreign authority for formulation of a request on international legal assistance in penal matters; 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.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or 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.	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 25 - Access to public, open sources** 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. 2. Foreign competent authority may have access to public, open Kosovar sources of computer data, without needing to file request to the Kosovar authorities.
Article 33 – Mutual assistance in the real-time collection of traffic data 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. 2 Each Party shall provide such assistance at least with respect to criminal	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 22 - Contact point** 1. In order to ensure a permanent international cooperation in the field of cyber crime, the Government shall make available a permanent contact point. 2. This permanent contact point possesses the following competencies: 2.1. provides specialized assistance and information on the legislation in the scope of cyber crime as well as informs contact points of other

offences for which real-time collection of traffic data would be available in a similar domestic case.	states; 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; 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.
Article 34 – Mutual assistance regarding the interception of content data 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.	**LAW ON INTERNATIONAL LEGAL COOPERATION IN CRIMINAL MATTERS** 1.Requests for international legal cooperation shall be transmitted through the Ministry of Justice. Where necessary, diplomatic channels may also be used. 2. In urgent cases, national judicial authorities may provide assistance even if the request is received directly, through INTERPOL, or in any other form which produces a written record, on condition that the requesting state assures that it will send the request in original within thirty (30)days in accordance with paragraph 1. of this Article.
Article 35 – 24/7 Network 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 domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 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.	**Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME** **Article 22 - Contact point** 1. In order to ensure a permanent international cooperation in the field of cyber crime, the Government shall make available a permanent contact point. 2. This permanent contact point possesses the following competencies: 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; 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; 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.

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. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	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.
Article 42 – Reservations 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.	The Republic of Kosovo has not ratified the Convention on Cybercrime (implemented through Law No.03/L –166 ON PREVENTION AND FIGHT OF THE CYBER CRIME)