Republika e Kosovës
Republika Kosovo-Republic of Kosovo
Kuvendi - Skupština – Assembly

Law No.03/L –166

ON PREVENTION AND FIGHT OF THE CYBER CRIME

Assembly of Republic of Kosovo,

Based on Article 65 (1) of Constitution of the Republic of Kosovo;

Approves

LAW ON PREVENTION AND FIGHT OF THE CYBER CRIME

Article 1
Objective

This Law aims to prevent and combat the cyber crime with concrete measures, prevent, discover and sanction violations through computer systems, by providing observance of the human rights and safeguard of the personal information.

Article 2
Scope

This Law applies to the territory of the Republic of Kosovo in the activities of computer systems. It is fully applicable to the preservation of data in computer systems as well as sanctions methods and procedures on how and by whom these data may be used.

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;

Article 5
Prevention, security and information campaigns

1. In order to ensure security for computer systems and protection of personal information, public authorities and institutions with competencies in this field, service providers, non-governmental organizations and representatives of civil society conduct activities and programs for prevention of the cyber crime.

2. Public authorities and institutions with competencies in this field in cooperation with service providers, non-governmental organizations and other representatives of civil society shall develop policies, practices, measures, procedures and minimum standards for security of computer systems.

3. Public authorities and institutions with competencies in this field in cooperation with service providers, non-governmental organizations and other representatives of civil society shall organize information campaigns on cyber crime and risks for the users of computer systems.

Article 6
Maintenance, supplementation and utilization of database

1. The Ministry of Justice in cooperation with the Ministry of Internal Affairs shall maintain and supplement continuously the database on cyber crime.

2. Ministry of Transport and Post-Telecommunications, Kosovo Intelligence Service and other relevant institutions can be users of the database in accordance with the rules and procedures of the database holder.

3. National Crime Institution shall carry out periodical studies in order to identify reasons and conditions that determine and favour the cyber crime.

Article 7
Special trainings and programs

The Ministry of Justice, Ministry of Internal Affairs, Ministry of Transport and Communications, Ministry of Public Services, Kosovo Intelligence Services shall develop special training programs to personnel for the purpose of preventing and fighting the cyber crime in accordance with the competencies they execute.

Article 8
Owner and administrator's obligations

1. For a category of computer systems, to which access is restricted or completely forbidden, the owners, administrators of this computer system are obliged to fix it by warning clearly and automatically the user: with information, as well as conditions of use, or forbiddance to use these computer system and legal consequences for unauthorized access to these computer systems.

2. Disobeying this obligation as determined under paragraph 1 of this Article, is violation and the perpetrator is fined in an amount from five hundred (500) € to five thousand (5000) € .

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 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 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 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 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.

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 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 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.

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 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.

Article 17
Prosecution procedure

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

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

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

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

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

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

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 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 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.

Article 20
International Cooperation

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

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

Article 21
Investigations

1. States and other organizations, upon their request could carry out investigation in cooperation with Kosovar authorities to prevent and fight cyber crime in the entire territory of Kosovo.

2. General investigations that refer to paragraph 1 of this Article are carried out on basis of bilateral and multilateral agreements.

3. The representatives of the competent Kosovar authorities may undertake investigations to be carried out in the territory of other countries in compliance with provisions of international agreements.

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.

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 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 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 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 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 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
Final Provisions

In case of discrepancies of the provisions of this Law with the provisions of the Code of Criminal Procedure the provisions of the Code of Criminal Procedure shall be applicable.

Article 28
Revenues

The revenues generated under this Law shall be deposited in the Budget of the Republic of Kosovo.

Article 29
Entry into force

This Law shall enter into force fifteen (15) days after its publication in the Official Gazette of the Republic of Kosovo.

Law No.03/L –166
10 June 2010

President of Assembly of the Republic of Kosovo

Jakup Krasniqi