Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version April 2008

Cybercrime legislation – country profile Estonia

This profile has been prepared within the framework of the Council of Europe's Project on Cybercrime 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:

Alexander Seger
Head of the Economic Crime Division
Department of Technical Cooperation
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:	**ESTONIA**
Signature of Convention:	23.11.2001
Ratification/accession: ***Provisions of the Convention***	12.05.2003 ***Corrresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data"	*National law including Penal Code uses the definitions of the Convention. Penal Code does not define these terms separately.*
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	Penal Code Art 217
Article 3 – Illegal interception	Penal Code Art 137
Article 4 – Data interference	Penal Code Art 206, Art 237
Article 5 – System interference	Penal Code Art 207, Art 237
Article 6 – Misuse of devices	Penal Code Art 216[1], Art 284

Article 7 – Computer-related forgery	Penal Code Art 344
Article 8 – Computer-related fraud	Penal Code Art 213
Article 9 – Offences related to child pornography	Penal Code Art 177, 178
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	Penal Code Art 219, 222, 222[1], 223, 224, 225, 225[1], 227
Article 11 – Attempt and aiding or abetting	Penal Code Art 20, 21, 22, 25, 26
Article 12 – Corporate liability	Penal Code Art 14
Article 13 – Sanctions and measures	Penal Code Art 44, 45, 46
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	
Article 15 – Conditions and safeguards	Constitution Art 26, 33, 43 Criminal Procedure Code Art 9, 64, 65, 110, 111, 112, 114, 121 Electronic Communications Act Art 102
Article 16 – Expedited preservation of stored computer data	Criminal Procedure Code Art 215 The obligations of a communication undertaking are regulated in Electronic Communications Act. Art 111[1] (in Estonian)
Article 17 – Expedited preservation and partial disclosure of traffic data	See comments on Article 16
Article 18 – Production order	Electronic Communications Act Art 112, 113
Article 19 – Search and seizure of stored computer data	Criminal Procedure Code Art 91, 126
Article 20 – Real-time collection of traffic data	Criminal Procedure Act 117 Electronic Communications Act Art 111[1], 112, 113
Article 21 – Interception of content data	Criminal Procedure Act Art 118 Electronic Communications Act Art 113
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	Penal Code Art 6, 7, 8, 9
Chapter III – International co-operation	
Article 24 – Extradition	Criminal Procedure Code Art 438, 439, 440

Article 25 – General principles relating to mutual assistance	Criminal Procedure Code Art 433, 435, 436, 437
Article 26 – Spontaneous information	Criminal Procedure Code Art 473
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	General principles apply. Criminal Procedure Code Art 433, 435, 436, 437
Article 28 – Confidentiality and limitation on use	General principles apply. Criminal Procedure Code Art 433, 435, 436, 437
Article 29 – Expedited preservation of stored computer data	General principles apply. Criminal Procedure Code Art 433, 435, 436, 437
Article 30 – Expedited disclosure of preserved traffic data	General principles apply. Criminal Procedure Code Art 433, 435, 436, 437
Article 31 – Mutual assistance regarding accessing of stored computer data	General principles apply. Criminal Procedure Code Art 433, 435, 436, 437
Article 32 – Trans-border access to stored computer data with consent or where publicly available	Criminal Procedure Code Art 64, 65
Article 33 – Mutual assistance in the real-time collection of traffic data	General principles apply. Criminal Procedure Code Art 433, 435, 436, 437
Article 34 – Mutual assistance regarding the interception of content data	General principles apply. Criminal Procedure Code Art 433, 435, 436, 437
Article 35 – 24/7 Network	24/7 contact point in Estonia is Central Criminal Police
Article 42 – Reservations	

Extracts from Estonian legislation

Constitution of the Republic of Estonia

§ 26.
Everyone has the right to the inviolability of private and family life. State agencies, local governments, and their officials shall not interfere with the private or family life of any person, except in the cases and pursuant to procedure provided by law to protect health, morals, public order, or the rights and freedoms of others, to combat a criminal offence, or to apprehend a criminal offender.

§ 33.
The home is inviolable. No one's dwelling, real or personal property under his or her control, or place of employment shall be forcibly entered or searched, except in the cases and pursuant to procedure provided by law, to protect public order, health or the rights and freedoms of others, to combat a criminal offence, to apprehend a criminal offender, or to ascertain the truth in a criminal procedure.

§ 43.
Everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means. Exceptions may be made by court authorisation to combat a criminal offence, or to ascertain the truth in a criminal procedure, in the cases and pursuant to procedure provided by law.

Penal Code

§ 6. Territorial applicability of penal law
(1) The penal law of Estonia applies to acts committed within the territory of Estonia.
(2) The penal law of Estonia applies to acts committed on board of or against ships or aircraft registered in Estonia, regardless of the location of the ship or aircraft at the time of commission of the offence or the penal law of the country where the offence is committed.

§ 7. Applicability of penal law by reason of person concerned
The penal law of Estonia applies to an act committed outside the territory of Estonia if such act constitutes a criminal offence pursuant to the penal law of Estonia and is punishable at the place of commission of the act, or if no penal power is applicable at the place of commission of the act and if:
1) the act is committed against a citizen of Estonia or a legal person registered in Estonia;
3) the offender is a citizen of Estonia at the time of commission of the act or becomes a citizen of Estonia after the commission of the act, or if the offender is an alien who has been detained in Estonia and is not extradited.
(2) The penal law of Estonia applies to an act committed outside the territory of Estonia if such act constitutes a criminal offence pursuant to the penal law of Estonia and the offender is a member of the Defence Forces performing his or her duties.

§ 8. Applicability of penal law to acts against internationally protected legal rights
Regardless of the law of the place of commission of an act, the penal law of Estonia shall apply to an act committed outside the territory of Estonia if the punishability of the act arises from an international agreement binding on Estonia.

§ 9. Applicability of penal law to acts against legal rights of Estonia
Regardless of the law of the place of commission of an act, the penal law of Estonia applies to acts committed outside the territory of Estonia if according to the penal law of Estonia the act is a criminal offence in the first degree and if such act:
1) causes damage to the life or health of the population of Estonia;
2) interferes with the exercise of state authority or the defence capability of Estonia, or
3) causes damage to the environment.

§ 14. Liability of legal persons
(1) In the cases provided by law, a legal person shall be held responsible for an act which is committed by a body or senior official thereof in the interest of the legal person.
(2) Prosecution of a legal person does not preclude prosecution of the natural person who committed the offence.
(3) The provisions of this Act do not apply to the state, local governments or to legal persons in public law.

§ 20. Offender
Offenders are principal offenders and accomplices.

§ 21. Principal offender
(1) Principal offender is a person who commits an offence unaided or by taking advantage of another person.
(2) If at least two persons agree to commit an offence jointly, each of them shall be held liable as a principal offender (joint principal offenders). An offence is deemed to be a joint offence also if an act committed by several persons jointly and in agreement comprises the necessary elements of an offence.

§ 22. Accomplice
(1) Accomplices are abettors and aiders.
(2) An abettor is a person who intentionally induces another person to commit an intentional unlawful act.
(3) An aider is a person who intentionally provides physical, material or moral assistance to an intentional unlawful act of another person.
(4) Unless otherwise provided by § 24 of this Code, a punishment shall be imposed on an accomplice pursuant to the same provision of law which prescribes the liability of the principal offender.
(5) In the case of an aider, the court may apply the provisions of § 60 of this Code.

§ 25. Attempt
(1) An attempt is an intentional act the purpose of which is to commit an offence.
(2) An attempt is deemed to have commenced at the moment when the person, according to the person's understanding of the act, directly commences the commission of the offence.
(3) If an act is committed by taking advantage of another person, the attempt is deemed to have commenced at the moment when the person loses control over the events or when the intermediary directly commences the commission of the offence according to the person's understanding of the act.

(4) In the case of a joint offence, the attempt is deemed to have commenced at the moment when at least one of the persons directly commences the commission of the offence according to the agreement of the persons.
(5) In the case of an omission, the attempt is deemed to have commenced at the moment when the person fails to perform an act which is necessary for the prevention of the consequences which constitute the necessary elements of an offence.
(6) In the case of an attempt, the court may apply the provisions of § 60 of this Code.

§ 26. Impossible attempt
(1) An attempt is impossible if it cannot be completed due to the unsuitability of the object or subject of the offence or due to the unsuitability of the object or method used to commit the offence.
(2) The court may release a person from punishment or apply the provisions of § 60 of this Code if due to his or her mental infirmity the person does not understand that the attempt is impossible.

§ 44. Pecuniary punishment
(1) For a criminal offence, the court may impose a pecuniary punishment of 30 to 500 daily rates.
(2) The court shall calculate the daily rate of a pecuniary punishment on the basis of the average daily income of the convicted offender. The court may reduce the daily rate due to special circumstances, or increase the rate on the basis of the standard of living of the convicted offender. The daily rate applied shall not be less than the minimum daily rate. The minimum daily rate shall be fifty kroons.
(3) Average daily income shall be calculated on the basis of the income subject to income tax received by the convicted offender during the year immediately preceding the year in which criminal proceedings were commenced against the convicted offender or, if the data pertaining to such year are not available, during the year preceding such year, less the income tax.
(4) Daily rates shall be calculated in full kroons.
(5) If at the time of commission of an act, the person is less than 18 years of age, the court may impose a pecuniary punishment of thirty up to two hundred and fifty daily rates. A pecuniary punishment shall not be imposed on a person of less than 18 years of age if he or she does not have any independent income.
(6) A pecuniary punishment may be imposed as a supplementary punishment together with imprisonment unless imprisonment has been substituted by community service.
(7) A pecuniary punishment shall not be imposed as a supplementary punishment together with a fine to the extent of assets.
(8) In case of a legal person, the court may impose a pecuniary punishment of fifty thousand to two hundred and fifty million kroons on the legal person. A pecuniary punishment may be imposed on a legal person also as a supplementary punishment together with compulsory dissolution.

§ 45. Imprisonment
(1) For a criminal offence, the court may impose imprisonment for a term of thirty days to twenty years, or life imprisonment.
(2) Imprisonment for a term of more than ten years or life imprisonment shall not be imposed on a person who at the time of commission of the criminal offence is less than 18 years of age.

§ 46. Compulsory dissolution of legal person
A court may impose the compulsory dissolution on a legal person who has committed a criminal offence if commission of criminal offences has become part of the activities of the legal person.

§ 137. Unauthorised surveillance
(1) A person without the lawful right to engage in surveillance who observes another person in order to collect information relating to such person shall be punished by a pecuniary punishment or up to 3 years' imprisonment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.

§ 177. Use of minors in manufacture of pornographic works
(1) Use of a person of less than 14 years of age as a model or actor in the manufacture of a pornographic or erotic picture, picture, film or other work, and use of a person of less than 18 years of age as a model or actor in the manufacture of a pornographic picture, film or other work is punishable by a pecuniary punishment or up to 5 years' imprisonment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.

§ 178. Manufacture of works involving child pornography or making child pornography available
(1) A person who manufactures, stores, hands over, displays or makes available in any other manner pictures, writings or other works or reproductions of works depicting a person of less than 18 years of age in a pornographic situation, or person of less than 18 years of age in a pornographic or erotic situation shall be punished by a pecuniary punishment or up to 3 years' imprisonment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.

§ 206. Interference in computer data
(1) Unlawful alteration, deletion, damaging or blocking of data or a program within a computer system, or unlawful entry of data or a program into a computer system is punishable by a pecuniary punishment or up to 3 years' imprisonment.
(2) The same act, if committed against a computer system of a vital sector (critical infrastructure) or if significant damage is thereby caused is punishable by a pecuniary punishment or up to 5 years' imprisonment.
(3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.

§ 207. Hindering of operation of computer system
(1) Unlawful interference or hindrance of the operation of a computer system by way of entry, transmission, deletion, damaging, alteration or blocking of data is punishable by a pecuniary punishment or up to 3 years' imprisonment.
(2) The same act, if significant damage is thereby caused, or the operation of a computer system of a vital sector (critical infrastructure) or the provision of public services is thereby hindered is punishable by a pecuniary punishment or up to 5 years' imprisonment
(3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.

§ 213. Computer-related fraud

(1) A person who receives proprietary benefits through unlawful entry, alteration, deletion, damaging or blocking of computer programs or data, or other unlawful interference with a data processing operation shall be punished by a pecuniary punishment or up to 5 years' imprisonment.

(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.

§ 216[1]. Preparation of computer-related crime

(1) A person who, for the purposes of committing the criminal offences provided in §§ 206, 207, 208, 213 or 217 of this Code prepares, possesses, disseminates or makes available in any other manner a device, program, password, protective code or other data necessary for accessing a computer system, or possesses, disseminates or makes available in any other manner the information necessary for the commission of the criminal offences specified in this section shall be punished by a pecuniary punishment or up to three years of imprisonment.

(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.

(3) A court may, pursuant to the provisions of § 83 of this Code, apply confiscation of an object which was the direct object of the commission of an offence provided for in this section.

§ 217. Unlawful use of computer system

(1) Unlawful access to a computer system by way of removal or circumvention of a code, password or other protective measure is punishable by a pecuniary punishment or up to 3 years' imprisonment.

(2) The same act, if:

1) it causes significant damage, or

2) is committed by using a computer system containing a state secret, classified foreign information or information prescribed for official use only, or

3) a computer system of a vital sector (critical infrastructure) has been accessed, is punishable by a pecuniary punishment or up to 5 years' imprisonment.

(3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.

§ 219. Violation of authorship

A person who discloses a work, performance of a work, an invention, industrial design or a layout-design of an integrated circuit of another in his or her own name shall be punished by a pecuniary punishment or up to 3 years' imprisonment

§ 222. Manufacture of pirated copy

(1) Reproduction, with the intention of distribution, of a work or an object of copyright without the permission of the author of the work, the holder of the copyright or the holder of the related rights is punishable by a pecuniary punishment or up to 3 years' imprisonment.

(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.

(3) The court shall confiscate the object which was the direct object of commission of an offence provided for in this section.

§ 222[1]. Possession of unlawfully reproduced computer programmes

(1) Unlawful physical use or possession of a computer programme for commercial purposes is punishable by a pecuniary punishment or up to 3 years' imprisonment.

(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
(3) The court shall confiscate the object which was the direct object of commission of an offence provided for in this section.

§ 223. Unlawful direction of works or objects of related rights towards public
(1) Unlawful public performance, showing, transmission, re-transmission or making available to the public or a work or an object of related rights for commercial purposes is punishable by a pecuniary punishment or up to one year of imprisonment.
(2) The same act, if performed by using a pirated copy, is punishable by a pecuniary punishment or up to 3 years' imprisonment.
(3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.
(4) The court shall confiscate the object which was the direct object of the offence provided for in subsection (2) of this section.

§ 224. Trade in pirated copies
(1) Trade in pirated copies, if a punishment for a misdemeanour has been imposed on the offender for the same act, is punishable by a pecuniary punishment or up to 3 years' imprisonment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
(3) The court shall confiscate the object which was the direct object of commission of an offence provided for in this section.

§ 225. Removal of technical means of protection preventing violation of copyright and related rights
(1) Unlawful removal of a of technical means of protection preventing violation of copyright and related rights, or manufacture, transfer or possession, or advertising for commercial purposes of a device or equipment intended for removal of such means of protection is punishable by a pecuniary punishment or up to 3 years' imprisonment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
(3) The court shall confiscate the object which was the direct object of commission of an offence provided for in this section.

§ 225[1]. Illegal receipt of information society services and broadcasting
(1) Manufacture for commercial purposes, transfer, installation, maintenance, possession or advertising of equipment or software enabling illegal access to fee-charging information society services or pay-TV or pay-radio programmes or broadcasts, or services enabling access to such services, programmes and broadcasts is punishable by a fine of up to 300 fine units.
(2) The same act, if committed by a legal person, is punishable by a fine of up to 50 000 kroons.

§ 227. Trade in counterfeit goods
(1) Trade in counterfeit goods is punishable by a pecuniary punishment or up to 3 years' imprisonment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.
(3) The court shall confiscate the object which was the direct object of commission of an offence provided for in this section.

§ 237. Acts of terrorism
(1) Commission of a criminal offence against international security, against the person or against the environment, or a criminal offence dangerous to the public posing a threat to life or health, or the manufacture, distribution or use of prohibited weapons, the illegal seizure, damaging or destruction of property to a significant extent or **interference in computer data** or **hindering of operation of computer system** as well as threatening with such acts, if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population is punishable by five to twenty years' imprisonment, or life imprisonment.
(2) The same act, if committed by a legal person, is punishable by compulsory dissolution.
(3) For the criminal offence provided in this section, the court shall impose extended confiscation of assets or property acquired by the criminal offence pursuant to the provisions of § 83^2 of this Code.

§ 284. Handing over protection codes
Unlawfully handing over the protection codes of a computer, computer system or computer network, if committed for the purpose of personal gain and in a manner which causes significant damage or results in other serious consequences is punishable by a pecuniary punishment or up to 3 years' imprisonment.

§ 344. Counterfeiting of documents, seals or blank document forms
(1) Counterfeiting a document, seal or blank document form on the basis of which it is possible to obtain rights or release from obligations is punishable by a pecuniary punishment or up to one year of imprisonment.
(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.

Criminal Procedure Code

§ 9. Safeguarding of personal liberty and respect for human dignity
(1) A suspect may be detained for up to forty-eight hours without an arrest warrant issued by a court.
(2) A person under arrest shall be immediately notified of the court's decision on arrest in a language and manner which he or she understands.
(3) Investigative bodies, Prosecutors' Offices and courts shall treat the participants in a proceeding without defamation or degradation of their dignity. No one shall be subjected to torture or other cruel or inhuman treatment.
(4) In a criminal proceeding, it is permitted to interfere with the private and family life of a person only in the cases and pursuant to the procedure provided for in this Code in order to prevent a criminal offence, apprehend a criminal offender, ascertain the truth in a criminal matter or secure the execution of a court judgment.

§ 64. General conditions for collection of evidence
(1) Evidence shall be collected in a manner which is not prejudicial to the honour and dignity of the persons participating in the collection of the evidence, does not endanger their life or health or cause unjustified proprietary damage. Evidence shall not be collected by

torturing a person or using violence against him or her in any other manner, or by means affecting a person's memory capacity or degrading his or her human dignity.
(2) If it is necessary to undress a person in the course of a search, physical examination or taking of comparative material, the official of the investigative body, the prosecutor and the participants in the procedural act, except health care professionals and forensic pathologists, shall be of the same sex as the person.
(3) If technical equipment is used in the course of collection of evidence, the participants in the procedural act shall be notified thereof in advance and the objective of using the technical equipment shall be explained to them.
(4) Investigative bodies and Prosecutors' Offices may involve impartial specialists in the collection of evidence and the specialists may be heard as witnesses.
(5) If necessary, participants in a procedural act shall be warned that pursuant to § 214 of this Code disclosure of information relating to pre-trial proceedings is prohibited.
(6) The general conditions for the collection of evidence by surveillance activities are listed in §§ 110–112 of this Code.

§ 65. Evidence obtained from foreign states
Evidence collected in a foreign state pursuant to the legislation of such state may be used in a criminal proceeding conducted in Estonia unless the procedural acts performed in order to obtain the evidence are in conflict with the principles of Estonian criminal procedure.

§ 91. Search
(1) The objective of a search is to find an object to be confiscated or used as physical evidence, a document, thing or person necessary for the adjudication of a criminal matter, property to be seized for the purposes of compensation for damage caused by a criminal offence or of confiscation, or a body, or to apprehend a fugitive in a building, room, vehicle or enclosed area.
(2) A search shall be conducted on the basis of an order of a Prosecutor's Office or a court ruling. The search of a notary's office or advocate's law office shall be conducted at the request of a Prosecutor's Office and on the basis of an order of a preliminary investigation judge or on the basis of a court ruling.
(3) In cases of urgency, an investigative body may conduct a search on the basis of an order of the investigative body without the permission of a Prosecutor's Office, but in such case the Prosecutor's Office shall be notified of the search within twenty-four hours and the Prosecutor's Office shall decide on the admissibility of the search.
(4) A search warrant shall set out:
1) the objective of the search;
2) the reasons for the search.
(5) A person may be searched without a search warrant:
1) in the event of detention of a suspect or arrest;
2) if there is reason to believe that the object to be found is concealed by the person at the place of the search.
(6) If a search is conducted, the search warrant shall be presented for examination to the person whose premises are to be searched or to his or her adult family member, or a representative of the legal person or the state or local government agency whose premises are to be searched, and he or she shall sign the warrant to that effect. In the absence of the appropriate person or representative, the representative of the local government shall be involved.
(7) A notary's office or an advocate's law office shall be searched in the presence of the notary or advocate. If the notary or advocate cannot be present at the search, the search shall be conducted in the presence of the person substituting for the notary or another advocate

providing legal services through the same law office, or if this is not possible, any other notary or advocate.
(8) If a search is conducted, the person shall be asked to hand over the object specified in the search warrant or to show where the body is hidden or the fugitive is hiding. If the proposal is not complied with or if there is reason to believe that the person complied with the proposal only partly, a search shall be conducted.

§ 110. Admissibility of surveillance activities in collection of evidence
(1) Evidence may be collected by surveillance activities in a criminal proceeding if collection of the evidence by other procedural acts is precluded or especially complicated and the object of the criminal proceeding is a criminal offence in the first degree or an intentionally committed criminal offence in the second degree for which at least up to three years' imprisonment is prescribed as punishment.
(1^1) Evidence may be collected by the surveillance activities specified in § 117 of this Code as a single inquiry on the conditions provided for in subsection (1) of this section in criminal proceedings commenced pursuant to § 120, 156, 157, 179 and 180, subsection 206 (1), § 207, subsection 208 (1), subsection 217 (1), §§ 245, 247, 249, 275, 305 and 323^1, subsection 377 (1) and § 398 of the Penal Code. For the purposes of this section, single inquiry is an inquiry for obtaining the information specified in subsection 117 (1) concerning a particular telephone call, a particular electronic mail, a particular electronic commentary or another communication session related to the forwarding of a single message.
(2) Evidence may be collected by the surveillance activities provided for in subsection (1) of this section also on the basis of an international request for assistance.

§ 111. Evidence obtained by surveillance activities
Information obtained by surveillance activities is evidence if such information has been obtained in compliance with the requirements of law.

§ 112. General conditions for collection of evidence by surveillance activities
(1) Surveillance activities shall not endanger the life, health or property of persons or the environment.
(2) Evidence is collected by surveillance activities by the Police Board and the Security Police Board on their own initiative or at the request of an investigative body. The Police Board collects evidence by surveillance activities directly or through the bodies administered by the Police Board. Evidence is collected by the surveillance activities specified in §§ 115 and 117 of this Code also by the Tax and Customs Board and Border Guard Administration.
(3) The permission of a preliminary investigation judge is necessary for the collection of evidence by the surveillance activities specified in §§ 116, 118 and 119 of this Code. The permission of a prosecutor who directs the proceedings is necessary for the collection of evidence by the surveillance activities specified in §§ 115 and 117 of this Code.
(4) If the conduct of surveillance activities is requested by another investigative body, the body which conducts the activities shall give written notification of the compliance with the request to the investigative body and, if necessary, send the photographs, films, audio and video recordings and other data recordings made in the course of the surveillance activities to the investigative body together with the surveillance report.
(5) A member of the Riigikogu or a rural municipality or city council, a judge, prosecutor, advocate, minister of religion or an official elected or appointed by the Riigikogu may be involved in surveillance activities with his or her consent and with the permission of a preliminary investigation judge only if a criminal offence is directed against him or her or a person close to him or her.

§ 114. Grant of permission for surveillance activities

(1) A preliminary investigation judge shall immediately review a reasoned request for the conduct of surveillance activities submitted by a prosecutor who directs the proceedings and grant or refuse to grant permission for the conduct of the surveillance activities by a ruling.

(2) Permission for surveillance activities is granted for up to two months and the permission may be extended by up to two months at a time at the request of a prosecutor who directs the proceedings.

(3) If covert entry into a dwelling or any other building or a vehicle, computer, computer system or computer network is necessary for the conduct of surveillance activities specified in §§ 115, 118 or 119 of this Code or in order to install or remove technical appliances necessary for the surveillance activities, separate permission shall be requested therefor pursuant to the procedure provided for in subsections (1)–(2) of this section.

(4) In cases of urgency, surveillance activities specified in §§ 116, 118 and 119 of this Code may be conducted without the permission specified in subsection (1) of this section on the basis of an order of the head of the Police Board, Central Criminal Police or the Security Police Board or an official appointed by him or her. The Prosecutor's Office shall immediately notify a preliminary investigation judge of the surveillance activities conducted and the judge shall decide on the admissibility of the activities and the grant of permission for continuation of the surveillance activities by a ruling.

§ 117. Collection of information concerning messages transmitted through commonly used technical communication channels

(1) Upon collection of information concerning messages transmitted by the public telecommunications network, information is collected from the operator of the electronic communications network or the provider of the postal or electronic communications service in order to ascertain the fact that a message has been transmitted, the duration and manner of transmission of the message, and the personal data and location of the sender or receiver.

(2) Information collected pursuant to the procedure provided for in subsection (1) of this section shall be recorded in the surveillance report.

§ 118. Wire tapping or covert observation of information transmitted through technical communication channels or other information

(1) Information obtained by wire-tapping or covert observation of messages or other information transmitted by the public electronic communications network shall be recorded and entered in the surveillance report.

(2) Information recorded upon wire-tapping or covert observation shall be entered in the surveillance report in so far as is necessary for the adjudication of the criminal matter.

(3) Information communicated by a person specified in § 72 of this Code which is subject to wire-tapping or covert observation shall not be used as evidence if such information contains facts which have become known to the person in his or her professional activities, unless the person has already given testimony with regard to the same facts or if the facts have been disclosed in any other manner.

§ 121. Submission of information collected by surveillance activities for examination

(1) A body which has conducted surveillance activities or the investigative body which requested the conduct of the surveillance activities shall immediately give notification of such activities to the person with regard to whom the activities were conducted and the persons whose private or family life was violated by the activities. With the permission of the

prosecutor, conduct of the surveillance activities need not be given notification of until the corresponding bases cease to exist if this may:
1) damage the rights and freedoms of another person which are guaranteed by law;
2) endanger the right of a person who has been recruited for surveillance activities to maintain the confidentiality of co-operation;
3) endanger the life, health, honour, dignity and property of an employee of a surveillance agency, a person who been recruited for surveillance activities or another person who has been engaged in surveillance activities and of persons connected with them;
4) prejudice a criminal proceeding or induce crime.
(2) At the request of a person specified in subsection (1) of this section, he or she is permitted to examine the materials of the surveillance activities conducted with regard to him or her, and the photographs, films, audio and video recordings and other data recordings obtained as a result of the surveillance. With the permission of the prosecutor, the following information may need not be submitted until the corresponding bases cease to exist:
1) information concerning the private life of other persons;
2) information the submission of which may damages the rights and freedoms of another person which are guaranteed by law;
3) information which contains state secrets or secrets of another person that are protected by law;
4) information the submission of which may endanger the right of a person who has been recruited for surveillance activities to maintain the confidentiality of co-operation;
5) information the submission of which may endanger the life, health, honour, dignity and property of an employee of a surveillance agency, a person who been recruited for surveillance activities or another person who has been engaged in surveillance activities and of persons connected with them;
6) information the submission of which may prejudice a criminal proceeding or induce crime;
7) information which cannot be separated or disclosed without information specified in clauses 1)-6) of this subsection becoming evident.

§ 126. Measures applicable to physical evidence and confiscated property
(1) Highly perishable physical evidence which cannot be returned to its lawful possessor shall be granted to a state or local government health care of social welfare institution free of charge, transferred, or destroyed in the course of the criminal proceeding on the basis of an order or ruling of the body conducting the proceedings. The money received from the sale shall be transferred into public revenues.
(2) Property subject to confiscation the lawful possessor of which has not been ascertained may be confiscated in the course of the criminal proceeding at the request of a Prosecutor's Office and on the basis of a court ruling.
(2^1) The property seized in order to secure confiscation may be transferred with the consent of the owner of the property and at the request of the Prosecutor’s Office on the basis of an order of a preliminary investigation judge. Property may be transferred without the consent of the owner if this is necessary for prevention of decrease in the value of the property. The amount received from transfer shall be seized.
(3) An order or ruling of the body conducting a proceeding or a court judgment shall prescribe the following measures applicable to physical evidence:
1) a thing bearing evidentiary traces of criminal offence, a document, or an impression or print made of evidentiary traces of a criminal offence may be stored together with the criminal matter, included in the criminal file or stored in the physical evidence storage facility or any other room in the possession of the body conducting the proceeding or in a forensic institution;

2) other physical evidence the ownership of which has not been contested shall be returned to the owner or lawful possessor thereof;
3) physical evidence of commercial value the owner or lawful possessor of which has not been ascertained shall be transferred into state ownership;
4) things of no value and pirated or counterfeit goods shall be destroyed or, in the cases provided by law, recycled;
5) objects which were used for staging a criminal offence shall be returned to the owners or lawful possessors thereof;
6) property which was obtained by the criminal offence and the return of which is not requested by the lawful possessor shall be transferred into state ownership or transferred in order to cover the costs of the civil action.
(4) If the ownership relations pertaining to physical evidence specified in clause (3) 2) of this section are not apparent, the measures applicable to the physical evidence in the pre-trial proceeding shall be decided by a ruling of the preliminary investigation judge at the request of the Prosecutor's Office.
(5) Subsections (1)–(3) of this section are applied also with regard to objects confiscated in a criminal proceeding which are not physical evidence.
(6) The procedure for the transfer and destruction of confiscated property and physical evidence transferred into state ownership and for the refund of the money received from the transfer to the lawful possessor of the property from the budget shall be established by the Government of the Republic.
(7) The procedure for registration, storage, transfer and destruction of physical evidence and seized property and for evaluation, transfer and destruction of highly perishable physical evidence by the bodies conducting the proceedings shall be established by the Government of the Republic.

§ 215. Obligation to comply with orders and demands of investigative bodies and Prosecutors' Offices
(1) The orders and demands issued by investigative bodies and Prosecutors' Offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia.
(2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately.
(3) A preliminary investigation judge may impose a fine of up to sixty minimum daily rates on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a Prosecutor's Office. The suspect and the accused shall not be fined.

§ 433. General principles
(1) International co-operation in criminal procedure comprises extradition of persons to foreign states, mutual assistance between states in criminal matters, execution of the judgments of foreign courts, taking over and transfer of criminal proceedings commenced, co-operation with the International Criminal Court and extradition to member states of the European Union.
(2) International co-operation in criminal procedure shall be effected pursuant to the provisions of this Chapter unless otherwise prescribed by the international agreements of the Republic of Estonia or the generally recognised principles of international law.

(3) International co-operation in criminal procedure shall be effected pursuant to the provisions of the other chapters of this Code in so far as this is not in conflict with the provisions of this Chapter.
(4) If adherence to the requirement of confidentiality is requested in the course of international co-operation in criminal procedure, such requirement shall be complied with to the extent necessary for the purposes of co-operation. If compliance with the confidentiality requirement is refused, the requesting state shall be immediately notified of such refusal.

§ 435. Judicial authorities competent to engage in international co-operation in criminal procedure
(1) The central authority for international co-operation in criminal procedure is the Ministry of Justice.
(2) Courts, Prosecutors' Offices, the Police Board, Security Police Board, Central Criminal Police, police prefectures, the Tax and Customs Board, Border Guard Administration, Competition Board and the Headquarters of the Defence Forces are the judicial authorities competent to engage in international co-operation in criminal procedure to the extent provided by law.
(3) If the Estonian Penal Code is applied to criminal offences which are committed outside the territory of the Republic of Estonia, the Public Prosecutor's Office, which initiates criminal proceedings or verifies the legality and justification of commencement of the criminal proceedings, shall be immediately informed thereof.

§ 436. Prohibition on international co-operation in criminal procedure
(1) The Republic of Estonia refuses to engage in international co-operation if:
1) it may endanger the security, public order or other essential interests of the Republic of Estonia;
2) it is in conflict with the general principles of Estonian law;
3) there is reason to believe that the assistance is requested for the purpose of bringing charges against or punishing a person on account of his or her race, nationality or religious or political beliefs, or if the situation of the person may deteriorate for any of such reasons.
(2) If a witness or expert is requested to be summoned to a foreign court, the request shall not be complied with if the requesting state fails to ensure compliance with the requirement of immunity on the bases provided for in § 465 of this Code.

§ 437. Division of expenses relating to international co-operation in criminal procedure
(1) The Republic of Estonia as the requesting and requested state shall bear all expenses incurred in its territory unless otherwise provided by an international agreement or a decision of the requested state.
(2) The Republic of Estonia as the requested state shall claim the following expenses from the requesting state:
1) expenses relating to the involvement of experts in Estonia;
2) expenses relating to the organisation of a hearing by telephone or video-conference in Estonia and to the attendance of the persons to be heard and the translators and interpreters unless otherwise agreed upon with the requesting state;
3) other essential or unavoidable expenses incurred by Estonia, to the extent agreed upon with the requesting state.
(3) On the basis of the request of a requesting state, the Estonian state may grant an advance to the experts and witnesses involved in international co-operation in criminal procedure.
(4) The Republic of Estonia as the requesting state shall bear all expenses incurred in the requested state if the expenses:

1) have arisen on the bases and pursuant to the procedure provided for in subsection (2) of this section;
2) are related to the transfer of a person in custody.

§ 438. Admissibility of extradition
Estonia as the requested state is entitled to extradite a person on the basis of a request for extradition if criminal proceedings have been initiated and an arrest warrant has been issued with regard to the person in the requesting state or if the person has been sentenced to imprisonment by a judgment of conviction which has entered into force.

§ 439. General conditions for extradition of persons to foreign states
(1) Extradition of a person for the purposes of continuation of the criminal proceedings concerning him or her in a foreign state is permitted if the person is suspected or accused of a criminal offence which is punishable by at least one year of imprisonment according to both the penal law of the requesting state and the Penal Code of Estonia.
(2) Extradition of a person for the purposes of execution of a judgment of conviction made with regard to him or her is permitted under the conditions provided for in subsection (1) of this section if at least four months of the sentence of imprisonment have not yet been served.
(3) If a person whose extradition is requested has committed several criminal offences and extradition is permitted for some of the criminal offences, extradition may be granted also for the other offences which do not meet the requirements specified in subsections (1) and (2) of this section.

§ 440. Circumstances precluding or restricting extradition of persons to foreign states
(1) In addition to the cases provided for in § 436 of this Code, extradition of a person to a foreign state is prohibited if:
1) the request for extradition is based on a political offence within the meaning of the provisions of the European Convention on Extradition and the Additional Protocols thereto;
2) the person has been finally convicted or acquitted on the same charges in Estonia;
3) according to the laws of the requesting state or Estonia, the limitation period for the criminal offence has expired or an amnesty precludes application of a punishment.
(2) Extradition of an Estonian citizen is not permitted if the request for extradition is based on a military offence within the meaning of the provisions of the European Convention on Extradition and the Additional Protocols thereto.
(3) If death penalty may be imposed in a requesting state as punishment for a criminal offence which is the basis for the request for extradition, the person may be extradited only on the condition that the competent authority of the requesting state has assured that death penalty will not be imposed on the person to be extradited or, if death penalty was imposed before the submission of the request for extradition, the penalty will not be carried out.
(4) A request for the extradition of a person to a foreign state may be denied if initiation of criminal proceedings on the same charges has been refused with regard to the person or if the proceedings have been terminated.

§ 473. Spontaneous information
Within the framework of mutual assistance in criminal procedure, a competent judicial authority may forward to a foreign state information obtained by a procedural act performed without prior request when such information may be the reason for initiating a criminal

proceeding in such foreign state or may assist in ascertaining the facts relating to a criminal offence subject to a criminal proceeding already initiated.

Electronic Communications Act

§ 102. General principles of data protection

(1) A communications undertaking is required to maintain the confidentiality of all information which becomes known thereto in the process of provision of communications services and which concerns subscribers as well as other persons who have not entered into a contract for the provision of communications services but who use communications services with the consent of a subscriber; above all, the following data must be protected:

1) specific data of using communications services;

2) the content and format of messages transmitted through the communications network;

3) information concerning the time and manner of transmission of messages.

(2) The information specified in subsection (1) of this section may be disclosed only to the relevant subscriber and, with the consent of the subscriber, to third persons, except in the cases specified in §§ 112, 113 and 114^1 of this Act. A subscriber has the right to withdraw his or her consent at any time.

(3) A communications undertaking may process the information provided for in subsection (1) of this section if the undertaking notifies the subscriber, in a clear and unambiguous manner, of the purposes of processing the information, and gives the subscriber an opportunity to refuse the processing.

(4) The obligation of a communications undertaking specified in subsection (3) of this section does not restrict the right of the undertaking to collect and process, without the consent of a subscriber, information which must be processed for the purposes of recording the transactions carried out in the conduct of business activities and for other business-related exchange of information. In addition to the above, the restriction provided in subsection (3) of this section does not limit the right of a communications undertaking to store or process data without the consent of a subscriber if the sole purpose of such activity is the provision of services through the communications network, or if such activity is necessary for the provision of the Information Society services defined by the Information Society Services Act which are directly requested for by the subscriber.

§ 111^1. Andmete säilitamise kohustus (Obligation to preserve data)

(1) Sideettevõtja on kohustatud säilitama andmed, et oleks võimalik teha järgmisi toiminguid:

1) sideallika seiramine ja tuvastamine;

2) side sihtpunkti tuvastamine;

3) side kuupäeva, kellaaja ja kestuse kindlaksmääramine;

4) sideteenuse liigi kindlaksmääramine;

5) sideteenuse kasutaja terminalseadme või oletatava terminalseadme kindlaksmääramine;

6) terminalseadme asukoha kindlaksmääramine.

(2) Telefoni- ja mobiiltelefoniteenuse ning telefonivõrgu ja mobiiltelefonivõrgu teenuse osutaja on kohustatud säilitama järgmised andmed:

1) helistaja number ning kliendi nimi ja aadress;

2) vastuvõtja number ning kliendi nimi ja aadress;

3) lisateenuse, sealhulgas kõne suunamise või edastamise kasutamise korral valitud number ning kliendi nimi ja aadress;

4) kõne alguse ja lõpu kuupäev ning kellaaeg;

5) kasutatud telefoni- või mobiiltelefoniteenus;

6) helistaja ja vastuvõtja rahvusvaheline mobiilside tunnus (*International Mobile Subscriber*

Identity – IMSI);
7) helistaja ja vastuvõtja rahvusvaheline mobiilside terminalseadme tunnus (*International Mobile Equipment Identity – IMEI*);
8) kärjetunnus kõne alustamise ajal;
9) andmed, mis määratlevad tugijaama geograafilise asukoha viitega kärjetunnusele ajavahemikul, mille jooksul andmeid säilitatakse;
10) anonüümse ettemakstud mobiiltelefoniteenuse korral teenuse esmase aktiveerimise kuupäev ja kellaaeg ning kärjetunnus, millest teenus aktiveeriti.
(3) Interneti-ühenduse, elektronposti ja Interneti-telefoni teenuse osutaja on kohustatud säilitama järgmised andmed:
1) sideettevõtja poolt eraldatud kasutajatunnused;
2) telefoni- või mobiiltelefonivõrku siseneva side kasutajatunnus ja telefoninumber;
3) kliendi nimi ja aadress, kelle nimele Interneti-protokolli aadress, kasutajatunnus või number olid side toimumise ajal eraldatud;
4) Interneti-telefoni kõne kavandatud vastuvõtja kasutajatunnus või number;
5) kavandatud vastuvõtva kliendi nimi, aadress ja kasutajatunnus elektronposti ning Interneti-telefoni teenuse korral;
6) Interneti-seansi alguse ja lõpu kuupäev ning kellaaeg konkreetse ajavööndi järgi koos Interneti-protokolli aadressiga, mille on kasutajale eraldanud Interneti-teenuse osutaja, ja kasutajatunnusega;
7) elektronposti või Interneti-telefoni teenuse kasutamise alguse (*log-in*) ja lõpu (*log-off*) kuupäev ning kellaaeg konkreetse ajavööndi järgi;
8) kasutatud Interneti-teenus elektronposti ja Interneti-telefoni teenuse korral;
9) helistaja number sissehelistamisega Interneti-ühenduse korral;
10) digitaalne kliendiliin (*Digital Subscriber Line – DSL*) või mõni muu tunnus side algataja kohta.
(4) Käesoleva paragrahvi lõigetes 2 ja 3 nimetatud andmeid säilitatakse üks aasta, alates side toimumise ajast, kui need sideteenuse osutamise käigus on loodud või neid on töödeldud. Käesoleva seaduse § 112 kohaselt esitatud järelepärimisi ja nende alusel antud teavet säilitatakse kaks aastat. Paragrahvi 112 alusel antud teabe säilitamise kohustus on järelepärimise esitajal.
(5) Käesoleva paragrahvi lõigetes 2 ja 3 nimetatud andmeid säilitatakse Euroopa Liidu liikmesriigi territooriumil. Eesti territooriumil säilitatakse:
1) käesoleva seaduse §-s 112 sätestatud järelepärimisi ja teavet;
2) käesoleva seaduse § 113 lõikes 5 nimetatud logifaile ja lõikes 6 sätestatud taotlusi;
3) käesoleva seaduse §-s 114^1 sätestatud üksikpäringuid.
(6) Avaliku korra ja riigi julgeoleku huvides võib Vabariigi Valitsus käesoleva paragrahvi lõikes 4 nimetatud tähtaega piiratud ajavahemikuks pikendada.
(7) Käesoleva paragrahvi lõikes 6 nimetatud juhul teavitab majandus- ja kommunikatsiooniminister sellest viivitamata Euroopa Komisjoni ja Euroopa Liidu liikmesriike. Kui Euroopa Komisjon ei ole kuue kuu jooksul pärast teavitamist oma seisukohta edastanud, loetakse lõikes 4 nimetatud tähtaeg pikendatuks.
(8) Käesoleva paragrahvi lõigetes 2 ja 3 nimetatud andmete säilitamise kohustust kohaldatakse ka ebaõnnestunud kõnede puhul, kui telefoni- ja mobiiltelefoniteenuse ning telefonivõrgu ja mobiiltelefonivõrgu teenuse osutamise korral vastavad andmed luuakse või neid töödeldakse. Nimetatud andmete säilitamise kohustust ei kohaldata kõnekatsele.
(9) Käesoleva paragrahvi lõigetes 2 ja 3 nimetatud andmete säilitamise korral peab sideettevõtja tagama:
1) sama kvaliteedi, turvalisuse ja andmekaitse nõuete täitmise, mida kohaldatakse teistele elektroonilise side võrgus olevatele analoogsetele andmetele;
2) andmete kaitse nende juhusliku hävimise või ebaseadusliku hävitamise, kadumise või

muutmise, loata või ebaseadusliku säilitamise, töötlemise, juurdepääsu või avalikustamise eest;
3) vajalikud tehnilised ja korralduslikud abinõud andmetele juurdepääsu piiramiseks;
4) side sisu kajastavate andmete säilitamata jätmise.
(10) Käesoleva paragrahvi lõigetes 2 ja 3 nimetatud andmete säilitamise või töötlemisega seonduvaid kulusid sideettevõtjale ei hüvitata.
(11) Käesoleva paragrahvi lõigetes 2 ja 3 nimetatud andmeid edastatakse ainult jälitus- või julgeolekuasutusele, Finantsinspektsioonile ja kohtule seaduses sätestatud korras.

§ 112. Obligation to provide information to surveillance agencies and security authorities

(1) Where adherence to the deadlines specified below is possible due to the nature of an enquiry, a communications undertaking is required to provide, within twenty four hours after receiving an urgent enquiry submitted by a surveillance agency or security authority, or within ten working days if the enquiry is not urgent, the surveillance agency or security authority with information at its disposal concerning:
1) information on the personal data of the sender and receiver of messages contained in the subscription contracts;
2) information on the location of the sender and recipient of messages;
3) the fact of transmission of messages, and the duration, mode and format of the messages;
4) the databases describing the transmission of messages in the process of message transmission and the data contained in the databases (the fact of transmission of messages, and the duration, mode and format of the messages).
(2) The enquiry specified in subsection (1) of this section shall be submitted in writing or by electronic media. Enquiries concerning messages specified in clause (1) 1) of this section may also be made in oral form verifying the request with a password. Access to the data specified in subsection (1) of this section may also be granted online on the basis of a written contract.

§ 113. Obligation to grant access to communications network

(1) Communications undertakings shall grant surveillance agencies and security authorities access to the communications network for the conduct of surveillance activities or for the restriction of the right to confidentiality of messages, correspondingly.
(2) In connection with granting a surveillance agency or security authority access to the communications network, the communications undertaking is required to submit information concerning the technical parameters of the communications network to the agency or authority, if they so request. A communications undertaking shall assume the obligation to immediately inform the surveillance agency or security authority of any modifications which are made to the technical parameters of the communications network and of the launching of any new services, if this may interfere with the performance of the obligations specified in subsection (3) of this section, and shall commence the performance of such obligations with regard to all offered services within a reasonable period of time.
(3) Upon granting access to a communications network, a communications undertaking is required to:
1) enable the surveillance agency or security authority to select messages and to ensure their transmission to a central or portable surveillance device of the surveillance agency or security authority in an unchanged form and in real time;
2) ensure the quality of message transmission which must be equal to the quality of the regular services provided by the communications undertaking;
3) ensure the protection of the messages and the data related to their transmission.

(4) Transmission by a communications undertaking of messages to a central or portable surveillance device of a surveillance agency or security authority shall be decided by the surveillance agency or security authority. A surveillance agency or security authority shall inform the Ministry of Economic Affairs and Communications of communications undertakings who transmit messages to central or portable surveillance devices of the surveillance agency or security authority.
(5) Transmission of messages to a central surveillance device shall be carried out by using a message splitting interface and appropriate hardware and software, which ensures the preservation of independent log files concerning the actions performed by the central surveillance device (time, type, object and number of action) for a period of at least five years.
(6) For transmission of messages to a portable surveillance device, a surveillance agency or security authority shall submit an application to a communications undertaking in writing or by electronic means for access to the communications network which shall set out the date, number and term of validity of the court order for the conduct of a surveillance activity or for the restriction of the confidentiality of messages. The communications undertaking is required to preserve such application for a period of at least five years.
(7) In the event of termination of the provision of communications services by a communications undertaking, the death, or dissolution of an undertaking, including as a result of merger or acquisition, or declaration of bankruptcy of a communications undertaking, the medium containing the log files specified in subsection (5) of this section and the applications specified in subsection (6) of this section shall be immediately transferred to the Communications Board. The procedure for preservation of log files and applications, transfer thereof to the Communications Board and for the transfer and destruction thereof shall be established by the Minister of Economic Affairs and Communications.
(8) In order to exercise supervision over the activities of surveillance agencies and security authorities, a Prosecutor's Office and the security authorities surveillance committee of the Riigikogu have the right to examine the applications specified in subsection (6) of this section and in the case of transmission of messages to a central surveillance device, also with the log files which are preserved.
(9) A communications undertaking is required to preserve the secrecy of information related to the conduct of surveillance activities, and activities which restrict the right to inviolability private life or the right to confidentiality of messages.
(10) Extraordinary and unavoidable acts necessary for enabling access to a communications network which interfere with the provision of communications services, as well as work performed by the undertaking on the communications network which interfere with the transmission of messages to the surveillance devices shall be performed under conditions agreed upon by the communications undertaking and the surveillance agency or the security authority in writing.