Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 30 May 2007
[Reformat in February 2011]

Cybercrime legislation – country profile

CZECH REPUBLIC

This profile has been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic 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:	**Czech Republic**
Signature of Convention:	9/2/2005
Ratification/accession:	
Provisions of the Convention	***Corresponding 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": 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	
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.	**Section 257a of the Criminal Code No140/1961 Coll. – subject to re-enactment** **Harming and Misusing Record on Data Carrier** (1) Whoever gains access to a data carrier and with intent to cause damage to another or to acquire unlawful benefit for himself or another, he a) unlawfully uses such data, b) damages, destroys, alters or renders useless such data, or c) interferes with the technical or program equipment or a computer or other telecommunication device, shall be sentenced to imprisonment of up to one year or prohibition of activity or pecuniary punishment or forfeiture of a thing or other property value. (2) An offender shall be sentenced to imprisonment of six months to three years if a) he commits the act given in paragraph 1 as a member of organized group, or b) he causes by such act substantial damage or acquires for himself or another substantial benefit.

	(3) An offender shall be punished by imprisonment of one year to five years if he causes by the act given in paragraph 1 extremely serious damage or acquires for himself or another large scale benefit
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.	**Section 239 of the Criminal Code No 140/1961 Coll. – subject to re-enactment** **Breach of Mailing Secrets** (1) Whoever intentionally breaches the secret of a) a sealed letter or other written document when providing postal or other transportation services, or b) massages transmitted by telephone, telegraph or other such public device, shall be sentenced to imprisonment of up to six months. (2) An employee of postal or telecommunication provider, who: a) commits an act given in paragraph 1, b) intentionally enables another to commit such crime, or c) alters or suppresses a written document in the post or transmitted by transport equipment, or a message transmitted by telephone, telegraph or other similar way, shall be sentenced to imprisonment of up to one year or prohibition of activity.
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.	**Section 257a, of the Criminal Code No 140/1961 Coll. – subject to re-enactment** **Harming and Misusing Record on Data Carrier** (1) Whoever gains access to a data carrier and with intent to cause damage to another or to acquire unlawful benefit for himself or another, he a) unlawfully uses such data, b) damages, destroys, alters or renders useless such data, or c) interferes with the technical or program equipment or a computer or other telecommunication device, shall be sentenced to imprisonment of up to one year or prohibition of activity or pecuniary punishment or forfeiture of a thing or other property value. (2) An offender shall be sentenced to imprisonment of six months to three years if a) he commits the act given in paragraph 1 as a member of organized group, or

	b) he causes by such act substantial damage or acquires for himself or another substantial benefit. (3) An offender shall be punished by imprisonment of one year to five years if he causes by the act given in paragraph 1 extremely serious damage or acquires for himself or another large scale benefit
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	**Section 257a of the Criminal Code No 140/1961 Coll. – subject to re-enactment** **Harming and Misusing Record on Data Carrier** (1) Whoever gains access to a data carrier and with intent to cause damage to another or to acquire unlawful benefit for himself or another, he a) unlawfully uses such data, b) damages, destroys, alters or renders useless such data, or c) interferes with the technical or program equipment or a computer or other telecommunication device, shall be sentenced to imprisonment of up to one year or prohibition of activity or pecuniary punishment or forfeiture of a thing or other property value. (2) An offender shall be sentenced to imprisonment of six months to three years if a) he commits the act given in paragraph 1 as a member of organized group, or b) he causes by such act substantial damage or acquires for himself or another substantial benefit. (3) An offender shall be punished by imprisonment of one year to five years if he causes by the act given in paragraph 1 extremely serious damage or acquires for himself or another large scale benefit
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	Criminal Code No 140/1961 Coll. – subject to re-enactment

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.	
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 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.	Not covered by the valid Criminal Code – subject to re-enactment
Article 8 – Computer-related fraud	**Sections 250 and 89 of the Criminal Code No 140/1961 Coll.**

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.	**Section 250 Fraud** (1)Whoever enriches himself or another person to the detriment of a property of another by misleading a person, or by taking advantage of another person's mistake or by withholding substantial facts, and thereby causes not insignificant damage to a property of another, shall be sentenced to imprisonment of up to two years, prohibition of activity, monetary punishment or forfeiture of a thing or other property value. (2)An offender shall be sentenced to imprisonment of six months to three years or monetary punishment if, by an act given in paragraph1, he causes not a small damage. (3) An offender shall be sentenced to imprisonment of two to eight years if: a) he commits the act given in paragraph 1 as a member of an organised group; or b) by such act he causes substantial damage or some other extremely serious consequence. (3) An offender shall be sentenced to imprisonment of five to twelve years if, by the act given in paragraph 1, he causes extremely serious damage. **Section 89** (1) „Crime" shall be understood as an act punishable in criminal proceedings and, unless a specific provision provides otherwise, also the preparation of a crime, an attempted crime, organisation, instigation and assistance. (2) „Act" shall also mean the omission of an act which the offender was obliged to perform according to the circumstances and his situation. (3) "Continuation of a crime" shall mean such conduct whose individual parts follow a common intent, thereby constituting the fact of a criminal act, and are associated by the same or a similar mode of commission and by close relation in time and in subject of attack.

	(4) A crime is committed publicly, if committed a) by the means of content of printed matter or distributed file, film, radio, TV broadcasting, or other similarly effective manner; or b) in the presence of two concurrently present persons. (5) A crime is committed with a weapon if the offender or, with his knowledge one of the accomplices, uses a weapon in an attack, to overcome or prevent resistance, or he has it on him for such purpose; a weapon shall be understood, unless provided otherwise in specific provision, as anything which makes a bodily attack more forcible. (6) A crime is committed violently if committed on person tricked into a condition of defencelessness as well. (7) Aggravated bodily harm shall mean serious impairment of health or serious illness. Under these conditions, aggravated bodily harm shall mean: a) disfigurement; b) loss or substantial diminution of capability to work; c) paralysation of a limb; d) loss or material reduction in the functioning of the sense organ; e) impairment of an important organ; f) mayhem; g) inducing abortion; h) excruciating anguish, or ch) long-term impairment of health. (8) A close person shall be understood as relative in direct line of descent, adoptive parent, adoptive child, sibling or spouse, partner; other persons in family or similar relation shell only be considered as close persons, when harm suffered by one of them is justifiably felt by the other as his own harm. (9) A public official is an elected official or other authorised employee of state authority or self-governing unit, court or other state body or a member of armed

	forces or security forces, judicial executor performing execution proceedings, listing of execution records and during proceeding performed on behalf of a court under special law, insofar he participates in the fulfilment of tasks for the society and the state, for which he exercises authority entrusted on him as part of his responsibility. When exercising power and authority under special laws a public official shall be understood a natural person appointed forest guard, nature guard, game-keeping guard or fishing guard. Criminal liability and protection of a public official under individual provisions of this law shall require that a crime is committed in connection with his authority and responsibility. The official or other responsible employee of a state authority or self-governing unit, armed forces or security forces of a foreign state are deemed as public officials under these conditions, if so stipulated by promulgated international treaty bound on the Czech Republic. (10) Addictive substance shall be understood as alcohol, narcotic substances, psychotropic substances and other substances capable of influencing adversely mind of a person or his ability to control or to recognize or his social behaviour. (11) Damage not insignificant shall be understood as damage amounting to at least 5 000 CZK, damage not small shall be understood as damage amounting to at least 25 000 CZK, a larger scope of damage shall be understood as damage amounting to at least 50 000 CZK, substantial damage shall be understood as damage amounting to at least 500 000 CZK and extremely serious damage shall be understood as damage amounting to at least 5 000 000 CZK. These amounts shall be used to determine the amount of profit, expenses on settlement of consequences of damage to the natural environment and value of a thing or other property value. (12) When determining the amount of damage, it shall be base on the price for which the thing - object of attack is usually sold at the place and time of such attack. If the amount of damage cannot be determined in such way, it shall be determined by efficiently spent funds on obtaining identical or similar thing or restoring it to its previous condition.

	(13) Thing shall also be understood as a controllable natural force. Provisions on things shall also relate to bonds and assets on bank account and provisions on immovable assets shall also relate to flats and non-residential premises, unless a specific provision indicates otherwise. Other property value shall be understood as property right or other value appraisable in money, which is not a thing. A thing or other property value belongs to the offender or other person if he owns it at the time of decision, or if he disposes with it as its owner, without knowing the real owner or possessor of such thing or other property value. (14) Burglary shall be understood as entering closed premises by trick, unlawfully forcing a lock or overcoming other security devices by force. (15) Where this Code connects effect with running of certain time, the day of a fact determining the beginning of such time period shall not be included in the period (16) For the purpose of this Criminal Code a natural person carrying out business activities under special law shall be considered an organisation. (17) Criminal conspiracy shall mean a group of several persons with its own internal organisational structure, with division of roles and distribution of activities that is aimed at systematic commission of intentional criminal activity. (18) To misrepresent or to use someone's mistake may also be achieved by interference with program equipment of a computer or execution of other computer operation, intervention with electronic or other technical equipment, including intervention with objects used to manage such devices provided with microchip, magnetic, optical or other special record, or by use of such operation or interference made by other person. (19) Insolvency administrator shall be understood also as provisional insolvency administrator, deputy of insolvency administrator, separated insolvency administrator, special insolvency administrator, bankruptcy trustee and settlement administrator. Insolvency administrator shall also be understood as

	person appointed pursuant to special legal regulation by insolvency administrator to represent him during execution of his powers according to special law on the territory of another state, further a foreign insolvency administrator, foreign insolvency administrator of insurance company or reinsurance company and person, appointed by the foreign insolvency administrator or foreign insolvency administrator of insurance or reinsurance company under special law to assist or represent him. (20) Insolvency proceedings shall be understood as proceedings according to the Act on Insolvency and Methods of Settlement (Insolvency Act) and to Act on Bankruptcy and Settlement.
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: 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	**Section 205 of the Criminal Code No 140/1961 Coll., full implementation subject to re-enactment** **Dissemination of Pornography** (1) Whoever, written, photographic, film, computerised, electronic or other such pornographic work a) offers, surrenders or makes accessible to a child, or b) displays or otherwise makes accessible in place accessible to children, shall be sentenced by imprisonment of up to two years, prohibition of activity or forfeiture of a thing or other property value. (2) Whoever produces, imports, exports, smuggles, offers, makes publicly accessible, mediates, put into circulation, sells or otherwise provides to other photographic, film, computerized, electronic or other pornographic work, a) depicting or otherwise using a child, b) depicting violence or disrespect to a human being, or c) depicting or otherwise representing sexual intercourse with animal, or who profits from such pornographic work, shall be sentenced to imprisonment of six months to three years, prohibition of activity, forfeiture of a thing or other property value. (3) An offender shall be sentenced to imprisonment of two years to six years if

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.	he commits an act given in paragraph 1 or 2 a) as a member of organized group, b) through press, film, radio or television broadcast, publicly accessible computer network or other similarly effective method, or c) with the intention to acquire substantial benefit for himself or another. (4) An offender shall be sentenced to imprisonment of three to eight years if he commits an act given in paragraphs 1 and 2 a) as a member of organized group operating in several countries, or b) with the intention to acquire large scale benefit for himself or another.
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 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	Czech Republic is party to the respective copyright conventions of the World Intellectual Property Organization, the provisions being implemented in the Copyright Code No 121/2000 Coll. Infringement of the rights thereof are subject to sanctions according to the Section 152 of the Criminal Code No 140/1961 Coll.

international instruments referred to in paragraphs 1 and 2 of this article.	
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.	
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.	Corporate liability has not yet been introduced into the Czech legislation
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be	Subject to new draft legislation

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 criminal or non-criminal sanctions or measures, including monetary sanctions.	
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. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether	

public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	Czech Republic has implemented the obligations from the fundamental international instruments on human rights
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of	**Section 84, art. 7 of the Telecommunication Code No 151/2000 Coll.** **Sections 90 and 97 of the Code on Electronic Communication No 127/2005 Coll.** **Section 90 Traffic Data** (1) Traffic data mean any data processed for the purposes of the transmission of a message via the electronic communications network or for the billing thereof. (2) The undertaking providing a public communications network or publicly available electronic communications service who processes and stores traffic data, including the appropriate location data relating to a user or subscriber, shall erase such data, or render them anonymous, once they are no longer

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.	needed for message transmission, except as provided in Subsections 3 and 4. The obligation of the legal entity or natural person providing a public communications network or a publicly available electronic communications service to maintain operating and location data according to Section 97 shall remain unaffected. (3) The undertaking providing a public communications network or publicly available electronic communications service may process the traffic data essential for the billing of the price for the service provided to a subscriber or user for access. Such processing is only admissible until the end of the period within which the billing of the price can be legally challenged or the payment thereof collected. Undertakings providing a public communications network or publicly available electronic communications service may provide each other with data related to the provision of the service, including, but not limited to, data about the subscribers being connected, in order to ensure interconnection and access to the network, mutual billing, and identification of any abuse of the electronic communications network and services. Abuse of electronic communications services means consistent late payment or non-payment of the billed price. (4) For the purposes of marketing the electronic communications services or for the provision of value-added services, the undertaking providing publicly available electronic communications service may only process the data referred to in Subsection 1 above to the extent and for the period as needed for such services or such marketing, as far as the subscriber or user to whom the data relate gave a consent thereto. The subscriber or user may withdraw his consent with the processing of traffic data at any time. (5) A value-added service means any service for which it is necessary to process traffic data – or location data other than those of traffic nature – beyond what is needed for the transmission of a message or for the billing thereof. (6) The undertaking providing publicly available electronic communications service shall inform the concerned subscriber or user about the traffic data being processed and about the time for which such data may be processed for the purposes referred to in Subsection 3. For the purposes referred to in Subsection 4, the undertaking shall so inform the subscriber or user to whom the data apply still before obtaining such a subscriber's or user's consent. (7) The undertaking providing a public communications network and the

	undertaking providing publicly available electronic communications service shall ensure that the traffic data processing according to Subsections 2 to 5 is restricted to a) the persons who were authorised to that effect by the that undertaking and who are responsible for the billing or operation management, for customer inquiries, fraud identification, electronic communications services marketing, or who provide value-added services; and b) the extent essential for the activities referred to in Clause a) above. **Section 97 Tapping and Recording Messages** (1) A legal entity or natural person providing a public communications network or publicly available electronic communications service shall, at the requesting party's expense, provide and secure interfaces at specified points of the network to connect terminal equipment for message tapping and recording: for the Police of the Czech Republic for purposes specified by a special legal regulation36. (2) In the course of message tapping or recording, the Police of the Czech Republic shall prove their authorisation for such activity by submitting a written application, which has a reference number under which a court decision is maintained and is signed by the person who is responsible for the performance of such activity. In the case of message tapping and recording on the basis of special legal regulations37 the written application shall contain the reference number under which the subscriber's consent is maintained. (3) A legal entity or natural person providing a publicly available communications network or electronic communications service shall store operating and location data and shall make such data available upon request to the bodies entitled to request them on the basis of a special legal regulation. The extent of such operating and location data, the time of the storage thereof, which shall not be longer than 12 months, and the form and manner of the handover thereof to the bodies entitled to use them, shall be specified in an implementing legal regulation. (4) A legal entity or natural person providing a publicly available telephony service shall, at the requesting party's expense, provide the Police of the Czech Republic upon their request with information from the database of all subscribers to the publicly available telephone service, the form and extent of such provision being specified by a special legal regulation.

	(5) Where a legal entity or natural person providing a public electronic communications network or publicly available electronic communications service introduces in its activities any coding, compression, encryption or any other method of transmission that makes the messages being transmitted icomprehensible, there such a person shall ensure that the requested messages and the traffic and location data related thereto are provided in a comprehensible manner at the termination points for connection of the terminal equipment referred to in Subsection 1. (6) For fulfilling the obligations specified in Subsections 1, 3 and 4 above, the legal entity or natural person is entitled to reimbursement for the efficiently incurred costs from the entitled entity that requested or ordered such an action. The amount of and method reimbursement for the efficiently incurred costs shall be specified in an implementing legal regulation. (7) The person referred to in Subsection 1 and its/his employees shall respect the confidentiality of the message tapping and recording requested and performed according to Subsections 3 and 4, including any circumstances relating thereto. (8) The technical and operating conditions and the points of connection of the terminal telecommunications equipment for message tapping and recording shall be specified in an implementing legal regulation. (9) A legal entity or natural person providing a publicly available communications network or electronic communications service shall be entitled to reimbursement for efficiently incurred costs from the entity upon whose request the legal entity or natural person provided information in accordance with Subsection 4 above. **Section 88a of the Code of Criminal Procedure No 141/1961 Coll.** **Police Act No 283/1991 Coll.** (1) If it is necessary, for the purposes of clarification of the circumstances significant for the criminal proceedings, to identify the data of the telecommunication traffic (transmissions) made, which are subject to the telecommunication secrecy or to which the protection of personal and mediation data applies, the chairman of panel (presiding judge), and the judge in the preparatory proceedings, shall order that the legal entities or natural persons

	performing the telecommunications services disclose these information to him, or to a public prosecutor or police agency in the preliminary proceedings. The order to identify the data of the telecommunication traffic must be issued in writing including its grounds (justification). (2) No order in accordance with subsection 1 is required if the user of the telecommunication device, which the data of the telecommunication traffic are to apply to, gives the consent to disclose the data.
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 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.	**Section 84, art. 7 of the Telecommunication Code No 151/2000 Coll.** **Sections 90 and 97 of the Code on Electronic Communication No 127/2005 Coll.** **Section 90 Traffic Data** (1) Traffic data mean any data processed for the purposes of the transmission of a message via the electronic communications network or for the billing thereof. (2) The undertaking providing a public communications network or publicly available electronic communications service who processes and stores traffic data, including the appropriate location data relating to a user or subscriber, shall erase such data, or render them anonymous, once they are no longer needed for message transmission, except as provided in Subsections 3 and 4. The obligation of the legal entity or natural person providing a public communications network or a publicly available electronic communications service to maintain operating and location data according to Section 97 shall remain unaffected. (3) The undertaking providing a public communications network or publicly available electronic communications service may process the traffic data essential for the billing of the price for the service provided to a subscriber or user for access. Such processing is only admissible until the end of the period within which the billing of the price can be legally challenged or the payment thereof collected. Undertakings providing a public communications network or publicly available electronic communications service may provide each other with data related to the provision of the service, including, but not limited to, data about the subscribers being connected, in order to ensure interconnection and access to the network, mutual billing, and identification of any abuse of the

	electronic communications network and services. Abuse of electronic communications services means consistent late payment or non-payment of the billed price. (4) For the purposes of marketing the electronic communications services or for the provision of value-added services, the undertaking providing publicly available electronic communications service may only process the data referred to in Subsection 1 above to the extent and for the period as needed for such services or such marketing, as far as the subscriber or user to whom the data relate gave a consent thereto. The subscriber or user may withdraw his consent with the processing of traffic data at any time. (5) A value-added service means any service for which it is necessary to process traffic data – or location data other than those of traffic nature – beyond what is needed for the transmission of a message or for the billing thereof. (6) The undertaking providing publicly available electronic communications service shall inform the concerned subscriber or user about the traffic data being processed and about the time for which such data may be processed for the purposes referred to in Subsection 3. For the purposes referred to in Subsection 4, the undertaking shall so inform the subscriber or user to whom the data apply still before obtaining such a subscriber's or user's consent. (7) The undertaking providing a public communications network and the undertaking providing publicly available electronic communications service shall ensure that the traffic data processing according to Subsections 2 to 5 is restricted to a) the persons who were authorised to that effect by the that undertaking and who are responsible for the billing or operation management, for customer inquiries, fraud identification, electronic communications services marketing, or who provide value-added services; and b) the extent essential for the activities referred to in Clause a) above. **Section 97 Tapping and Recording Messages** (1) A legal entity or natural person providing a public communications network or publicly available electronic communications service shall, at the requesting party's expense, provide and secure interfaces at specified points of the network to connect terminal equipment for message tapping and recording: for the Police of the Czech Republic for purposes specified by a special legal regulation36. (2) In the course of message tapping or recording, the Police of the Czech

	Republic shall prove their authorisation for such activity by submitting a written application, which has a reference number under which a court decision is maintained and is signed by the person who is responsible for the performance of such activity. In the case of message tapping and recording on the basis of special legal regulations37 the written application shall contain the reference number under which the subscriber's consent is maintained. (3) A legal entity or natural person providing a publicly available communications network or electronic communications service shall store operating and location data and shall make such data available upon request to the bodies entitled to request them on the basis of a special legal regulation. The extent of such operating and location data, the time of the storage thereof, which shall not be longer than 12 months, and the form and manner of the handover thereof to the bodies entitled to use them, shall be specified in an implementing legal regulation. (4) A legal entity or natural person providing a publicly available telephony service shall, at the requesting party's expense, provide the Police of the Czech Republic upon their request with information from the database of all subscribers to the publicly available telephone service, the form and extent of such provision being specified by a special legal regulation. (5) Where a legal entity or natural person providing a public electronic communications network or publicly available electronic communications service introduces in its activities any coding, compression, encryption or any other method of transmission that makes the messages being transmitted icomprehensible, there such a person shall ensure that the requested messages and the traffic and location data related thereto are provided in a comprehensible manner at the termination points for connection of the terminal equipment referred to in Subsection 1. (6) For fulfilling the obligations specified in Subsections 1, 3 and 4 above, the legal entity or natural person is entitled to reimbursement for the efficiently incurred costs from the entitled entity that requested or ordered such an action. The amount of and method reimbursement for the efficiently incurred costs shall be specified in an implementing legal regulation. (7) The person referred to in Subsection 1 and its/his employees shall respect the confidentiality of the message tapping and recording requested and performed according to Subsections 3 and 4, including any circumstances relating thereto. (8) The technical and operating conditions and the points of connection of the

	terminal telecommunications equipment for message tapping and recording shall be specified in an implementing legal regulation. (9) A legal entity or natural person providing a publicly available communications network or electronic communications service shall be entitled to reimbursement for efficiently incurred costs from the entity upon whose request the legal entity or natural person provided information in accordance with Subsection 4 above. **Section 88a of the Code of Criminal Procedure No 141/1961 Coll.** **Police Act No 283/1991 Coll.** (1) If it is necessary, for the purposes of clarification of the circumstances significant for the criminal proceedings, to identify the data of the telecommunication traffic (transmissions) made, which are subject to the telecommunication secrecy or to which the protection of personal and mediation data applies, the chairman of panel (presiding judge), and the judge in the preparatory proceedings, shall order that the legal entities or natural persons performing the telecommunications services disclose these information to him, or to a public prosecutor or police agency in the preliminary proceedings. The order to identify the data of the telecommunication traffic must be issued in writing including its grounds (justification). (2) No order in accordance with subsection 1 is required if the user of the telecommunication device, which the data of the telecommunication traffic are to apply to, gives the consent to disclose the data.
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.	**Sections 78, 79, 88 and 158d of the Code of Criminal Procedure No. 141/1961 Coll.** **Section 78 Liability to deliver a thing** (1) Anyone possessing a thing important for the criminal proceedings is obliged to submit the thing to the court, public prosecutor or police body based on call; if it is necessary to secure the thing for the purpose of criminal proceedings, the person is obliged to deliver the thing to the bodies on call. Upon the call it is necessary to notify the person that if he/she fails to meet the call the thing can be taken away from him/her as well as other consequences of the failure to meet the obligation (Section 66). (2) The obligation under paragraph 1 does not apply to the written instrument

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 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.	the content of which relates to a circumstance for which prohibition of examination applies unless the release from the obligation to keep the matter confidential or release from the duty of non-disclosure has taken place (Section 99). (3) The presiding judge is authorised to call for deliver of a thing; the public prosecutor or police body are authorised to do so in pre-trial proceedings. **Section 79 Seizure of a thing** (1) If the thing necessary for criminal proceedings is not issued on call by the person possessing the thing, it can be taken away based on order of the presiding judge and in pre-trial proceedings based on order of the public prosecutor or police body. The police body needs a prior consent of the public prosecutor for the issue of such order. (2) If the body that issued the order to take away the thing does not execute the taking away itself, it shall be executed by the police body based on the order. (3) The police body may issue the order without prior consent specified in paragraph 1 provided only that the prior consent cannot be achieved and the act must be performed immediately. (4) A person not participating in the matter shall be eventually engaged in taking away of the thing. (5) The report on delivery and taking away of a thing must also include a sufficiently accurate description of the thing delivered or taken away to allow for identification thereof. (6) The person that delivered the thing or from which the thing was taken away shall be immediately given a written acknowledgement of acceptance of the thing or copy of the report by the body that carried out the act. **Section 47 of the Police Act No 283/1991 Coll.** **Telecommunication Code No 151/2000 Coll.** (1) When performing their tasks, the police departments are entitled to request from the state and municipal authorities, legal entities and natural persons their assistance in the performance of the departments' tasks, in particular, the necessary background materials and information. The provision of section 12 (3) through (5) shall apply accordingly. (2) The authorities, entities and persons referred to in paragraph (1) must provide the requested assistance, unless the execution and observance of their

	duties under other generally binding legal regulations prevents that. (3) Police departments shall notify the authorities, entities and persons referred to in paragraph (1) of the facts which may affect their work and may lead to endangering or breaching public order or to a threat to the security of persons or property.
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. 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,	**Sections 82 – 85b of the Code of Criminal Procedure No 141/1961 Coll.** **Section 82** **Reasons for house searches and personal searches and searches of other premises and plots of land** (1) A house search may be carried out if there are grounds for suspicion that a thing or person important for criminal proceedings is in a flat or other premises used for residence or in premises belonging to them (residence). (2) A search of non-residential premises (other premises) and plots of land may also be carried out for the reasons specified in paragraph 1, if they are not accessible to the public. (3) A personal search may be carried out if there are grounds for suspicion that the person has an thing important for criminal proceedings on his/her person. (4) A personal search may also be carried out on a person detained and on a person who has been arrested or who is being taken into custody if it is suspected that he/she is carrying a weapon or other thing which could endanger his/her own or another person's life or health. **Section 83** **Search warrant** (1) Presiding judge and in pre-trial proceedings the judge based on motion of the public prosecutor are authorised to order the search of close premises. In exigent cases this can be done by the presiding judge or the judge, in the district of whom the search is to be carried out, instead of the appropriate presiding judge or judge (Section 18). The search warrant must be issued in writing and justified. It shall be served on the person, in the premise of whom the search is to be carried out, during the search, and if this is not possible, within 24 hours at the latest from elimination of the obstacle preventing from the service. (2) A search warrant shall be executed upon order of presiding judge or judge

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.	by a police body. **Section 83a** **Warrant for a search of other premises and plots of land** (1) A search warrant for other premises or plots of land is authorised by the presiding judge, and in pre-trial proceedings the state prosecutor or the police authority. The police authority requires previous consent of the state prosecutor. The warrant must be issued in writing and reasons must be given. It is delivered to the user of the premises or plots of land concerned, and, if he/she is not found in the search, immediately after the impediment which prevents delivery is removed. (2) A search of other premises or plots of land is carried out by the authority which ordered it or the police authority at its order. (3) The police may only carry out a search of other premises or plots of land without a warrant or the consent specified in paragraph 1 if the warrant or consent could not be obtained in advance and the matter cannot be delayed, or if the user of the premises or plots of land concerned declares in writing that he/she consents to the search and delivers its declaration to the police authority. The authority which is authorised to issue the warrant or consent specified in paragraph 1 must be informed of this action promptly. **Section 83b** **Personal search warrant** (1) A personal search warrant is authorised by the presiding judge and in pre-trial proceedings by the state prosecutor or with his/her consent the police authority. (2) If the personal search is not carried out by the authority which ordered it, it is carried out by the police authority at its order. (3) A personal search is always carried out by a person of the same sex. (4) The police may only carry out a personal search without a warrant or consent specified in paragraph 1 if the warrant or consent could not be obtained in advance and the matter could not be delayed, or if it involves a person caught in the act or a person for whom an arrest warrant has been issued. A personal search may also be carried out without a warrant or consent in the cases specified in Section 82 para. 4.

	Section 83c **Entry to dwellings, other premises and plots of land** (1) The police may only enter dwellings, other premises or plots of land if the matter cannot be delayed and entry is necessary to protect persons' lives or health or protect other rights and freedoms or avert serious danger to public security and order. (2) They may also enter places specified in paragraph 1 if an arrest warrant or a writ of attachment or a committal warrant for a person living there has been issued. (3) No actions other than those serving to eliminate an imminent danger or to deliver a person may be carried out during entry to places specified above. **Section 84** **Preliminary questioning** A house search or personal search or search of other premises and plots of land may only be carried out after preliminary questioning of the person on whose premises or against whom this action is to be carried out, only if voluntary delivery of an thing sought or elimination of another reason which led to this action has not been achieved by questioning. Preliminary questioning is not required if the matter cannot be delayed and questioning cannot take place immediately. **Carrying out searches and entry to dwellings, other premises and plots of land** **Section 85** (1) The authority carrying out a house search or search of other premises is obliged to enable the person at whose premises this action is carried out or any adult member of his/her household, or in the case of a search of other premises also employees, to participate in the search. It is obliged to instruct these persons of their right to participate in the search. (2) For carrying out a house and a personal search it is necessary to co-opt a person who is not involved in the matter. The authority carrying out the search shows its authorisation. (3) In the search protocol it is also necessary to state whether the provisions on previous questioning have been observed, or to give the reasons why they were not observed. If a thing has been delivered or seized in a search, it is also necessary to incorporate data specified in Section 79 para. 5 in the protocol.

	(4) The authority which executed this action provides the person on whose premises the search was carried out with a written confirmation of the result of the action, and also take-over of things which were delivered or seized in it, immediately, and if this is not possible, within 24 hours at the latest, or provides a copy of the protocol. (5) In entry to dwellings, other premises and plots of land, the provisions of paragraphs 1 to 4 are used as appropriate. However, participation of persons specified in paragraph 1 in entry to dwellings and co-opting of a person specified in paragraph 2 can be refused, if this could lead to endangering his/her life or health. **Section 85a** (1) The person on whose premises a house search, a search of other premises and plots of land, a personal search or entry to dwellings is to be carried out is obliged to bear with this search. (2) If the person against whom an action specified in paragraph 1 is aimed does not enable this action to be carried out, the authorities carrying out the action are authorised, when a previous appeal has proved fruitless, to override this person's opposition or the impediment created by him/her. This is recorded in the protocol (Section 85 para. 3). **Section 85b** (1) When carrying out a house search or search of other premises, where a solicitor carries out his legal profession, and where documents with information covered by solicitor's duty of non-disclosure could be found, the law enforcement authority is obliged to seek cooperation of the Czech Bar Association ("Association"); the body carrying out the search is entitled to be acquainted with the content of documents only in the presence and with consent of a representative of the Association, who is nominated by the President of the Association from its employees or from solicitors. The position of the representative of the Association shall be stated in the protocol (Section 85 para. 3). (2) If the representative of the Association refuses to grant the consent under para 1, the documents shall be secured in the presence of the law enforcement authority, solicitor and representative of the Association in such a way, so that nobody shall be able to be acquainted with them, eventually destroy or damage them; these documents shall immediately be handed over to the Association.

	The Association shall return them to the solicitor without delay if the time to file a petition under par. 5 expires; the Association proceeds accordingly in case the petition was rejected, including some documents; in such case the Association returns documents rejected by the petition. The Association returns the documents to the solicitor without delay when it was informed about the procedure under par. 6. (3) In cases under par. 2, first sentence, the consent of the representative of the Association may be replaced, based on the proposal of the authority which authorised the house search or search of other premises, by decision of a judge of immediate superior court, to which the president of panel or a judge who is authorised to order a house search or search of other premises under sec. 83 para. 1 and sec. 83a para. 1. Same is applicable to search of other premises conducted by police authority under sec. 83a para. 3; in such case the warrant is issued by the president of panel and in preliminary proceedings by the state attorney. (4) In addition to general elements (sec. 59 para. 4), the petition must contain the designation of documents regarding which the petitioner is seeking the replacement of consent of the Association's representative with acquainting with documents and stating of the facts proving the reason why the disapproval of the Association's representative should be replaced with the decision of a judge based on para. 3. Protocol reporting the disapproval of the Association's representative shall be included to the petition. (5) The petition shall be submitted in 15 days from the day that the representative of the Association denied the consent with acquainting with documents, regarding which the petitioner is seeking the replacement of consent of the Association's representative under para. 4 (6) The judge shall not consider petition which does not contain all elements, or which is incomprehensible or indefinite, provision of sec. 59 par. 4 sent. three and four shall not be used. The judge shall decide accordingly if the petition was submitted with delay or by a person not authorised to petition. The judge informs the petitioner and the Association of the measure without delay. (7) Unless the judge proceeds according to par. 6, he considers the petition without delay in open session and imposes to the Association to submit the relevant documents. Apart other acts, the judge examines whether the security of documents submitted by the Association was not violated, and gets acquainted with the content; at the same time he takes measures not to allow the petitioner or anybody else to learn the content of documents during the

	open session. (8) If the open session is suspended, the judge shall secure the documents not to allow anybody to become acquainted with the content, eventually to destroy or damage them. (9) The judge shall grant the consent if he draws the conclusion that the document does not content facts covered by the concerned solicitor's duty of non disclosure; failing which he rejects the petition. (10) If the judge satisfies the petition in part he hands over the respective documents without delay following the legal force of the judicial resolution by which the consent of the Association's representative was replaced to the authority executing the act and imposes on him to return documents to the Association immediately after he will get acquainted with the content; this is not applicable if the documents shall be used as evidence in criminal proceedings. Documents, regarding which the petition was rejected, shall be returned to the Association by the judge without delay following the legal force of the judicial resolution. (11) In case the documents can not be surrendered to the authority carrying out the act, Association or its representatives in person, they shall be delivered on the first working day following the day on which the judicial resolution came into legal force at the latest, to the authority carrying out the act or the Association by judicial deliverer of by the body of Judicial Guard. (12) Documents in paras. 1 to 11 are understood as written material, or its part, as well as other data carrier.
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	**Section 88 of the Code of Criminal Procedure No 141/1961 Coll.** article not implemented completely **Section 88** (1) If criminal proceedings are conducted for an especially serious intentional crime or for any other intentional crime the prosecution of which is an obligation resulting from a promulgated international treaty, the presiding judge and in pre-trial proceedings the judge based on motion of the public prosecutor may order to intercept and record the telecommunication operation (traffic, transmissions) provided that there is a justified assumption that any fact significant for the criminal proceedings would be communicated through it. It is not allowed to execute any interception or record of telecommunication operation between (defence) counsel and the charged person. If the police body

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.	ascertains from the interception and records of the telecommunication operation that the charged person communicates with his/her counsel, the police body is obliged to discontinue the intercepting immediately, destroy the record of the contents, and abstain from using in any way the information it has gained in this connection. (2) An order to intercept and record telecommunication traffic shall be issued in written form and justified. At the same time the period of interception and recording of telecommunication traffic must be stipulated, which can not be longer then 6 months with possibility of (repeated) prolongation for another 6 months by judge. Judge immediately forwards the copy of an order to a public prosecutor. The Police of the Czech Republic carries out interceptions and recordings of the telecommunication operations (traffic) for the purposes (needs) of all bodies active in (responsible for) the criminal proceedings. (3) Without an order under the subsection 1 of this provision the agency can order an interception and recording of the telecommunication operations or carry out it itself even in the cases not mentioned in the subsection 1, if a user of tapped telecommunication station agrees. (4) If the tapping and registration of telecommunication traffic is to be used as an evidence, it is necessary to attach to it the protocol with the data on the place, time, ways and content of registration, and about the person who made the recording as well. Other records shall be marked and reliably archived; it is necessary to write down in the protocol attached to file where the record is archived. It is possible to use as an evidence the record of telecommunication traffic in another criminal case than in the case in relation to which the record has been made if a prosecution in this another case is conducted also for criminal offence mentioned in subsection 1 of this provision or if user of tapped telecommunication station agrees. (5) If during the interception and recording of telecommunication traffic no facts important for criminal proceedings were find out, it is necessary to destroy the records in prescribed way.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be	**Section 88 of the Code of Criminal Procedure No 141/1961 Coll.** article not implemented completely

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.	(1) If criminal proceedings are conducted for an especially serious intentional crime or for any other intentional crime the prosecution of which is an obligation resulting from a promulgated international treaty, the presiding judge and in pre-trial proceedings the judge based on motion of the public prosecutor may order to intercept and record the telecommunication operation (traffic, transmissions) provided that there is a justified assumption that any fact significant for the criminal proceedings would be communicated through it. It is not allowed to execute any interception or record of telecommunication operation between (defence) counsel and the charged person. If the police body ascertains from the interception and records of the telecommunication operation that the charged person communicates with his/her counsel, the police body is obliged to discontinue the intercepting immediately, destroy the record of the contents, and abstain from using in any way the information it has gained in this connection. (2) An order to intercept and record telecommunication traffic shall be issued in written form and justified. At the same time the period of interception and recording of telecommunication traffic must be stipulated, which can not be longer then 6 months with possibility of (repeated) prolongation for another 6 months by judge. Judge immediately forwards the copy of an order to a public prosecutor. The Police of the Czech Republic carries out interceptions and recordings of the telecommunication operations (traffic) for the purposes (needs) of all bodies active in (responsible for) the criminal proceedings. (3) Without an order under the subsection 1 of this provision the agency can order an interception and recording of the telecommunication operations or carry out it itself even in the cases not mentioned in the subsection 1, if a user of tapped telecommunication station agrees. (4) If the tapping and registration of telecommunication traffic is to be used as an evidence, it is necessary to attach to it the protocol with the data on the place, time, ways and content of registration, and about the person who made the recording as well. Other records shall be marked and reliably archived; it is necessary to write down in the protocol attached to file where the record is archived. It is possible to use as an evidence the record of telecommunication traffic in another criminal case than in the case in relation to which the record has been made if a prosecution in this another case is conducted also for criminal offence mentioned in subsection 1 of this provision or if user of tapped

	telecommunication station agrees. (5) If during the interception and recording of telecommunication traffic no facts important for criminal proceedings were find out, it is necessary to destroy the records in prescribed way.
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 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.	**Sections 16 to 20A of the Criminal Code No 140/1961 Coll.** **§ 16** (1) The liability to punishment for an act shall be considered according to the Act (law) in force at the time when the act was committed; it shall be considered under a subsequent Act only if consideration under such law is more favorable to the offender. (2) Only such punishment can be imposed upon an offender as may be imposed under the Act in effect at the time when a verdict on the criminal offence is made. (3) Protective measures shall be decided under the Act in effect at the time when the decision is taken. **§ 17** (1) The liability to punishment for a criminal offence committed on the territory of the Czech Republic shall always be considered under the law of the Czech Republic. (2) A criminal offence shall be considered as having been committed on the territory of the Czech Republic a) if an offender acted on its territory, even if the violation of, or threat to, an interest protected under this Code resulted, or was to result, completely or partly abroad, or b) if an offender violated or threatened on its territory an interest protected under this Code, or if the consequence of such a criminal offence was to have occurred on its territory at least partly, even though the criminal offence was

	committed abroad. (3) The liability to punishment for a criminal offence committed outside the territory of the Czech Republic on board a ship (vessel) or an aircraft registered in the Czech Republic shall also be considered under the law of the Czech Republic. The place where the criminal offence in question is committed shall be considered similarly as in case falling under par. 2. **§ 18** The liability to punishment for an act committed abroad by a citizen of the Czech Republic or by a stateless person (a person having no citizenship) authorized to reside permanently in the Czech Republic shall also be considered under Czech law. **§ 19** The Czech law shall apply when determining punishability for subversion of the Republic (§ 92), terror (§ 93 and 93a), diversion (§ 95 and 96), sabotage (§ 97), espionage (§ 105), the counterfeiting and altering of means of currency (§ 140), the placing of counterfeit and altered means of currency (money) into circulation (§ 141), manufacture and possession of counterfeiting tools (§ 142), assault on a state authority under § 153 and assault on a public official under § 155, genocide (§ 259), use of a forbidden weapon and non-permitted conduct of war (§ 262), cruelty in war (§ 263), persecution of citizens (§ 263a), plunder in an area of military operations (§ 264), abuse of internationally-recognized and state insignia (§ 265) and a crime against peace under § 1 of the Peace Protection Act, No. 165/1950 Coll., even if such a criminal offence was committed abroad by a foreign national or a stateless person who does not reside (i.e. has no permanent permit to reside) on the territory of the Czech Republic. **§ 20** (1) The Czech law shall be applied to determine the punishability for an act committed abroad by a foreigner (i.e. a citizen of another state) or a stateless person who is not authorized to reside permanently on the territory of the Czech Republic a) if the act is also punishable under the law in force on the territory where it was committed, and

	b) if the offender is apprehended on the territory of the Czech Republic and was not extradited for criminal prosecution to a foreign state. (2) However, such offender shall not be sentenced to a more severe punishment than that stipulated under the law of the state on whose territory the criminal offence was committed. **§ 20a** (1) The punishability for an act shall also be considered under Czech law in cases stipulated in a promulgated international convention (agreement, treaty) which is binding on the Czech Republic. (2) The provisions of § 17 – 20 shall not apply if it is not admitted under a promulgated international agreement binding on the Czech Republic.
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 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 each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual	Implemented through ratification of the relevant international instruments

assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in 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.	
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	Implemented through ratification of the relevant international instruments, i.e. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990) and Criminal Law Convention on Corruption (1999)

provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
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. 6 Before refusing or postponing assistance, the requested Party shall,	To be in effect upon ratification

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	To be in effect upon ratification

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 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 for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.	To be in effect upon ratification

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.	
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 involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic	To be in effect upon ratification

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.	
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.	To be in effect upon ratification
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.	To be in effect upon ratification
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	To be in effect upon ratification

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 offences for which real-time collection of traffic data would be available in a similar domestic case.	
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.	To be in effect upon ratification
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. 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.	To be in effect upon ratification
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.	