

Project on Cybercrime

www.coe.int/cybercrime



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

First draft (30 May 2007)

Cybercrime legislation – country profile

Slovakia

This profile has been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Alexander Seger
Department of Technical Cooperation
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	Slovakia
Signature of Convention:	4.2.2005
Ratification/accession:	No Convention on Cyber Crime is now in final stage of legislative process. By the end of 2007 it is expected to be submitted to National council of the Slovak Republic for ratification.
Provisions of the Convention	Corresponding provisions/solutions in national legislation <i>(pls quote or summarise briefly; pls attach relevant extracts as an appendix)</i>
<i>Chapter I – Use of terms</i>	
Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”	SEC. 247 of the Criminal Code Act no 300/2005 Coll.
<i>Chapter II – Measures to be taken at the national level</i>	
<i>Section 1 – Substantive criminal law</i>	
Article 2 – Illegal access	SEC. 247 (1) of the Criminal Code Act no 300/2005 Coll.
Article 3 – Illegal interception	SEC. 247 (2) a of the Criminal Code Act no 300/2005 Coll.
Article 4 – Data interference	SEC. 247 (1) b, d of the Criminal Code Act no 300/2005 Coll.
Article 5 – System interference	SEC. 247 (1) d of the Criminal Code Act no 300/2005 Coll.
Article 6 – Misuse of	SEC. 247 (1) c of the Criminal Code Act no 300/2005 Coll.

devices	
Article 7 – Computer-related forgery	SEC. 247 (1) d of the Criminal Code Act no 300/2005 Coll.
Article 8 – Computer-related fraud	SEC. 226 of the Criminal Code Act no 300/2005 Coll.
Article 9 – Offences related to child pornography	SEC. 368-370 of the Criminal Code Act no 300/2005 Coll.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	SEC. 283 of the Criminal Code Act no 300/2005 Coll.
Article 11 – Attempt and aiding or abetting	SEC. 14 (1), 20, 21(1)d of the Criminal Code Act no 300/2005 Coll.
Article 12 – Corporate liability	(See note no 1 below)
Article 13 – Sanctions and measures	For the art 13(1) of Convention on Cybercrime - SEC. 196,247,369,283 of the Criminal Code Act no 300/2005 Coll.
<i>Section 2 – Procedural law</i>	
Article 14 – Scope of procedural provisions	SEC. 90,118 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 15 – Conditions and safeguards	SEC.14-25 of SK Constitution, SEC. 90,118 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 16 – Expedited preservation of stored computer data	SEC. 90 (1)a of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 17 – Expedited preservation and partial disclosure of traffic data	SEC. 90 (1)a, b, e of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 18 – Production order	SEC. 90 (1)e, 118 (3) of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 19 – Search and seizure of stored computer data	SEC. 91 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 20 – Real-time collection of traffic data	SEC. 90 (1)a, b, e of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 21 – Interception of content data	SEC. 90 of the Code of Criminal Procedure Act no 301/2005 Coll.
<i>Section 3 – Jurisdiction</i>	
Article 22 – Jurisdiction	SEC. 3 of the of the Criminal Code Act no 300/2005 Coll.
<i>Chapter III – International co-operation</i>	
Article 24 – Extradition	SEC. 498-514 of the Code of Criminal Procedure Act no 301/2005 Coll. (See note no 2 below)
Article 25 – General principles relating to mutual assistance	SEC. 1(2) of the SK Constitution, SEC. 531-537 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 26 – Spontaneous information	SEC. 484 of the Code of Criminal Procedure Act no 301/2005 Coll.

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	SEC. 479 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 28 – Confidentiality and limitation on use	SEC. 482 (2) of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 29 – Expedited preservation of stored computer data	SEC. 551 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 30 – Expedited disclosure of preserved traffic data	SEC. 551 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 31 – Mutual assistance regarding accessing of stored computer data	SEC. 537 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 32 – Trans-border access to stored computer data with consent or where publicly available	SEC. 537 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 33 – Mutual assistance in the real-time collection of traffic data	SEC. 537 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 34 – Mutual assistance regarding the interception of content data	SEC. 537 of the Code of Criminal Procedure Act no 301/2005 Coll.
Article 35 – 24/7 Network	(See note no 3 below)
Article 42 – Reservations	

Appendix 1: **Solutions in national legislation of the Slovak Republic.**

There is no *expressis verbis* definition of the "computer system", "computer data", "service provider", "traffic data" in the SK Criminal Code Act no. 300/2005, Coll., but, for the purposes of the Criminal Code, following terms and sentences/phrases are used:

"*Computer*" may be described as functional unit performing calculation of any numerical and logical operation without human interference and following specific program.

"*Information carrier*" means material carrier of information, in particular hard disc, floppy disc (diskette), CD-Rom, cassette of a tape-recorder etc.

"*Unauthorized access to an information carrier*" is any acting which enables/permits free disposal with the carrier of information or possibly with a part of it as well as use of the information contained in it.

"*Interference with the technical or program equipment of a computer*" means any interference with the technical equipment of a computer including its accessories, i.e. interference with the computer unit itself, keyboard, monitor, printer etc. (so-called hardware) or interference into program or its part (so-called software).

"*Obstructing/hindering of computer system*" is actually destruction of the original computer data by any of the forms stated in the law.

Pursuant to the Section 130, par. 2 SK Criminal Code (Act no. 300/2005, Coll.) also non-material information, computer technique data or image recorded in technical carrier is considered as thing.

Basic bodies of a crime concerning the acts mentioned have the following wording in **the Criminal Code of the Slovak Republic** (and relevant provisions):

Section 247

Damaging and misusing a record in the information carrier

(1) Any one shall be liable to a sentence of deprivation of liberty for six months up to three years, who obtains/gains unauthorized access to a computer system or to other information carrier or to a part of it with the intent to cause a damage or any other prejudice to another, or to obtain undue advantage for himself or for another and who

- a) shall make unauthorized use of an information contained there
- b) destroys, damages, deletes, alters or reduces/worsens a quality of an information in it
- c) interferes with the technical or program equipment of a computer, or
- d) enters, transfers/transmits, damages, deletes, reduces quality, alters or restraints/suppresses the computer data in order to obstruct/hinder the functionality/operation of a computer system, or who creates unauthentic data with the intent such data are deemed authentic or used so for legal purposes.

(2) The same sentence as referred to in the par. 1 shall be imposed to any one who for the purpose of a criminal offence described in the par. 1

- a) without authorization and by means of technical devices shall watch/monitor a non public/close transfer of computer data into a computer system, from it or within it, or

- b) procures/obtains or makes access to a computer program or other devices, to a computer password, access code or any similar data permitting/enabling access to whole/entire computer system or to its part.

Section 226

Undue enrichment

(1) Any one shall be liable to a sentence of deprivation of liberty up to two years who by means of unauthorized interference with the technical or program equipment of a computer, automate, or any other similar device serving for automatic sale of goods, exchange or withdrawal of money or for providing automatic and paid performance, services, or for any other performance obtains/acquires goods, services or information without required payment or who obtains a money illegally and enriches himself or another to a prejudice of another person's property causing a small damage to another persons' property.

Section 368

Production/manufacturing child pornography

(1) Any one shall be liable to a sentence of deprivation of liberty for four up to ten years who makes use, offers or otherwise abuses a child for the purpose of producing child pornography or who permits/allows for such abuse or who participates in such production any other manner.

Section 369

Distribution of child pornography

(1) Any one shall be liable to a sentence of deprivation of liberty for one up to five years who reproduces, transports, procures, makes access to or otherwise distributes child pornography.

Section 370

Sheltering/storing child pornography

Any one shall be liable to a sentence of deprivation of liberty for up to two years who stores/conceals child pornography.

Section 283

Breach of copyright

(1) Any one shall be liable to a sentence of deprivation of liberty for maximum term of two years who unlawfully interferes with the legally protected rights to a work, artistic performance, audio record or audio and video record, broadcasting or televising or to a database.

Section 14

Attempted crime

(1) Attempted crime means an acting which directly aims to completing a commission of a criminal offence and which was committed by a perpetrator if a criminal offence was not completed.

(2) Attempted crime is punishable according to a severity of sentence imposed for completed criminal offence.

Section 20

Accomplice

If a criminal offence was committed by joint acting of two or more perpetrators (accomplices), each one of them is accountable for it like he/she would have committed it alone.

Section 21

Participant in a crime (accessory)

(1) A person is considered/deemed a participant in a completed or attempted crime if he/she intentionally

- a) plotted or directed commission of a crime (organizer)
- b) counseled another to commit a crime (abettor)
- c) requested another to commit a crime (orderer), or
- d) assisted another in committing a crime, in particular by procuring means, removing obstacles, counseling/advising, strengthening resolution, promising assistance in committing a crime (aider, assisting offender).

(2) Provisions about criminal responsibility of a perpetrator shall apply to the criminal responsibility of a participant in a crime unless provided otherwise in this Act.

note no 1:

The Slovak Republic has not implemented the criminal responsibility of legal entities in its criminal codes so far. Nowadays, legal entities may be sanctioned only within the scope of administrative law.

Section 31

Punishment and protective measure

(1) Pursuant to this Act, punishments and protective measures are sanctions that represent consequence in law of a criminal offence committed or of an act otherwise punishable.

(2) Sanction means detriment/prejudice to personal freedom, property or other rights of a convict; only a court may impose them for committed criminal act pursuant to this Act.

(3) Protective measure means a detriment/prejudice to a personal freedom or to a property of a convict or of another person; only a court may impose such measure in the interest of protecting the society against criminal offences or against acts otherwise punishable.

Section 32

Types of punishments

For the criminal acts committed, a court may impose only the following punishments to a perpetrator who is natural person:

- a) deprivation of liberty
- b) house arrest
- c) compulsory work
- d) pecuniary punishment
- e) forfeiture/confiscation of property
- f) forfeiture/confiscation of a thing
- g) prohibition to undertake professional activities
- h) prohibition of abode
- i) deprivation of titles and honors
- j) deprivation of a military rank and other rank
- k) banishment.

Section 33

Types of protective measures

There are the following protective measures:

- a) protective medical treatment
- b) protection in a young offender institutions

- c) protective supervision
- d) detention
- e) seizure of a thing.

Relevant provisions of the Code of Criminal Procedure of the Slovak Republic

Section 90

Storing and delivering (handing over) of computer data

(1) If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings, then presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of:

- a) storing and keeping completeness of such data
- b) enabling production and keeping/possession of copies of such data
- c) making access to such data impossible
- d) removing from computer system such data
- e) handing over such data for the purposes of criminal proceedings.

(2) The order issued pursuant to the par. 1 must state a period of time during which data storage shall be carried out, maximum period is 90 days, and if repeated storage is necessary, new order shall be issued.

(3) If storage is no longer necessary of computer data including traffic data for the purposes of criminal proceedings, presiding judge or prosecutor in the stage before the commencement of criminal prosecution or within pre-trial proceedings shall issue the order to cancel data storage without delay.

(4) An order issued pursuant to the par. 1 to 3 shall be served on a person in whose possession or control the data are or to a service provider of such services; both of them may be imposed the obligation of keeping in secret the measures contained in the order.

Section 91

Seizure of a thing

(1) If upon a demand a person fails to render a thing or computer data that are material for criminal proceedings, then - upon an order issued by a presiding judge or a by prosecutor within pre-trial proceedings or by a police officer - such thing may be seized to a person. Prior consent by a prosecutor is necessary for the police for issuing such order.

(2) If the authority issuing the order to seize does not execute itself a seizure of a thing, the police shall execute it upon an order.

(3) Police may issue an order without prior consent pursuant to the par. 1 only in the event where prior consent is impossible to be given and the matter is urgent.

(4) If possible, the unparticipating person shall be involved in the seizure of a thing.

(5) A person or service provider who is in possession/control of the computer data or of information about the services concerned shall hand over/deliver them to a person who had issued the order pursuant to the par. 1.

Section 118

Comparison of data found in different computer systems

(1) Comparison of data within different information systems containing characteristic/typical or excluding features of persons or things material for criminal proceedings may be carried out if necessary for clarification of a crime within criminal proceedings on willful criminal act liable to a sentence of deprivation of liberty with the maximum term exceeding 3 years, on corruption or on any other willful crime if such proceedings are to be conducted pursuant to a binding international treaty.

(2) Written order to compare data in different information systems shall be issued by presiding judge or by prosecutor within proceedings prior to commencement of criminal prosecution or within pre-trial proceedings.

(3) An order issued pursuant to the par 1 shall contain name of information system operator who is obliged to hand over the data as well as definition of data and also testing data that are necessary for comparison.

(4) A person defined in the par. 3 is obliged to provide data necessary for the comparison. If the data requested are inseparable from other data, then other data shall be handed over as well. Such other data may not be used as evidence.

(5) If data were provided in an information carrier, they shall be returned back immediately after termination of a comparison. Data transferred to other information carriers shall be immediately destroyed by that law enforcement officer/court/police officer who carried out the comparison, if such data are not longer necessary for criminal proceedings.

(6) If a record made from data comparison is to be used as evidence, the procedure shall be carried out pursuant to the Section 115 accordingly.

(7) Record may be used as evidence in another criminal matter different from that one within which a comparison had been made only if there is simultaneous criminal proceedings conducted in that matter concerning some of the criminal acts as referred to in the par. 1.

(8) If no material facts are found for criminal proceedings as result of comparison, then that law enforcement authority/court/police which had carried out the comparison, shall immediately destroy the record obtained and he shall do it in prescribed manner.

Section 3 (SK Criminal Code)

Territorial competence/jurisdiction

(1) Pursuant to this Act, the punishability of an act committed in the territory of the Slovak Republic shall be examined.

(2) A criminal act is deemed/considered to be committed in the territory of the Slovak Republic even in the case where the offender

- a) committed the act partially in the SK territory, if breach or endangering of an interest protected by this Act has occurred or should/might occur either entirely or partially in the territory of the Slovak Republic, or
- b) committed an act outside SK territory if breach or endangering of an interest protected by this Act should occur here, or if such consequence might occur here even partially.

(3) Pursuant to this Act, punishability of an act shall also be examined if committed outside SK territory on board of a ship flying the Slovak flag or on board of an aircraft recorded in the Aircraft Register of the Slovak Republic.

note no 2:

In whole its extent, the SK domestic/internal regulation corresponds with the Article 24, Convention on Cybercrime. Within the extradition proceedings, the Slovak authorities proceed according to the provisions of the section 489 to 514, of the Code of Criminal Procedure of the Slovak Republic, as well as international treaties by which the Slovak Republic is bound and also pursuant to the rules of international law.

Corresponding provisions of the Constitution of the Slovak Republic (Act no. 460/1992, Coll.)

Article 1

(2) Slovak Republic recognizes and observes general rules of international law, international treaties by which it is bound as well as its further international commitments.

Article 7

(2) By means of an international treaty ratified and promulgated in a legal manner, or on the basis of such treaty, the Slovak Republic may transfer to the European Communities and to the European Union one part of its own rights. Legally binding acts of both the European Communities and of the European Union take precedence over the laws of the Slovak Republic. Adoption of legally binding acts requiring implementation shall be carried out by means of a law or governmental decree pursuant to the Article 120, par. 2.

(3) With the aim of maintaining peace, security and democratic order and according to the terms stipulated by an international treaty, the Slovak Republic may join an organization of mutual collective security.

(4) Prior to the ratification, the consent by the National Council of the Slovak Republic is required for the validity of any international treaty on human rights and fundamental freedoms, international political treaties, international treaties with military nature, international treaties establishing membership of the Slovak Republic in international organizations, international economic treaties of general nature, international treaties for the implementation/execution of which a laws is necessary, and of any international treaty directly establishing rights or duties of natural persons or of legal entities.

(5) International treaties on human rights and fundamental freedoms, international treaties for the execution of which no law is necessary as well as international treaties directly establishing rights or duties of natural persons or of legal entities and that had been ratified and promulgated in legally stipulated manner take precedence over laws.

Relevant provisions of the Code of Criminal Procedure in the Slovak Republic:

Section 479

Mutuality/reciprocity

(1) If a requesting country is not bound by an international treaty then the Slovak authorities may handle its request if a requesting country shall guarantee that it shall handle similar request by the Slovak authority, and if handling/execution of a foreign country's request is not bound/conditioned by existence of international treaty. Fulfilment of the condition stated in the first sentence shall not be examined in the case of foreign authority's request for service of a document on a person in the territory of the Slovak Republic.

(2) If a requested country that is not bound by an international treaty, requests mutuality/reciprocity as a condition for executing the Slovak authority's request, then the Ministry of Justice may give reciprocity guarantee to the requested country as for handling similar request by requested country and upon a condition that no international treaty existence is required for carrying out such request.

Section 482

Protection and use of information

(2) Slovak authorities shall not publish nor provide/furnish no information nor evidence obtained from foreign authority on the basis of a request made according to this Part or in connection with it, and they shall not use it for any other purpose but that one for which they had been sent or requested if they are bound so by an international treaty or if the information and evidence was provided to them only upon promise of fulfillment of this condition; this does not apply if a foreign authority gives consent with publication or with any other use of information or evidence.

Section 484

Sending requests for information by means of Interpol

(1) Pursuant to this Part, requests may be sent to foreign country as well as received from it also by means of International Criminal Police Organization (hereinafter referred to as "Interpol"), in particular in the cases of urgent matters.

(2) By means of Interpol, also information and data may be exchanged concerning the time and further details in relation to the transfer, taking over or transport of a person or thing pursuant to the Section 485.

Spontaneous information exchange is regulated also in the Article 7, Convention on Mutual Assistance in Criminal Matters between EU Countries drawn up by the Council in accordance with the Article 34, Treaty Establishing the European Union (Notifications by the Ministry of Foreign Affairs, no. 572/2006, Coll.).

Requests made by foreign authorities

Section 537

Method and form of handling a request

(1) Slovak authorities shall execute a request made by foreign authorities in a manner stipulated by this Act or by an international treaty. If mutual assistance is made pursuant to an international treaty in a manner that is not regulated in this Act, then a competent prosecutor shall decide on a method of executing legal assistance.

(2) Upon request by foreign authority, the requested legal assistance may be executed pursuant to the legal rule of requesting country unless the requested procedure is contrary to the interests protected by the provision of the Section 481.

(3) In order to execute a request pursuant to the Section 539, par. 1, it is required that the act in relation to which the request is made, should be criminal act not only pursuant to the legal order of the requesting country, but also pursuant to the legal order of the Slovak Republic.

Explanatory comments on the provision of the Section 537, Code of Criminal Procedure of the Slovak Republic (extract):

The mentioned provision explicitly expresses the basic principle of executing legal assistance pursuant to the law of the requested country (lex fori).

It regulates the extent/scope of the legal assistance awarded so that it restricts/limits it by means of legal regulation of this Act or an international treaty. Upon request by foreign authorities, competent SK authorities may execute in principle any act they are competent to carry out within criminal proceedings conducted in the Slovak Republic or any act regulated by an international treaty. Extent of mutual assistance so defined is also limited by the following elements:

- *in absence of international treaty, actual reciprocity is a prerequisite of carrying out legal assistance i.e. competent authorities of the requesting country are expected to provide the same type of legal assistance as they are requesting for in a similar case,*
- *execution of some specific legal assistance acts is conditioned by contractual reciprocity (Section 544, 551), the execution of them is excluded in absence of contractual regulation,*
- *no significant protected SK interest shall be hindered through execution of requested acts (section 481).*

If requesting authority requests execution of an act pursuant to an international treaty by which SK is bound, whilst the requested method is not regulated in this Act, competent prosecutor shall decide on a manner/method of execution of legal assistance act (Section 538, par.2).

If requesting authority requests for execution of an act on the basis of an international treaty containing regulation of specific procedure/method that is more detailed or different from domestic legal order regulation, then the act shall be executed pursuant to the international treaty and competent prosecutor shall decide on modalities of carrying out of the act (Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters).

The provision of the par. 2 admits/allows execution of the legal assistance act pursuant to the legal order of a foreign country, unless such method is contrary to the important protected interests of the Slovak Republic (Section 481) that represents breaching of the basic principle lex fori.

In such case, competent prosecutor is obliged to submit to the court a request for decision pursuant to the Section 539, par. 2. Court shall decide on existence, absence of conflict with the interests protected by the Section 481 and it shall define method of execution of the act.

In the event that an act is executed pursuant to the legal rules of a foreign country without court decision made pursuant to the Section 539, par. 2, such act is considered as executed contrary to the SK legal regulation.

Par. 3: Existence of dual criminality in general does not represent condition of realization of legal assistance carrying out the request.

Provision regulates exception to this rule in the cases where court order is required for producing evidence.

Examination of dual criminality is conditioned by the fact that it concerns acts representing interference with human rights and fundamental freedoms and the realization of such acts is limited by court decision within criminal proceedings on criminal act. In the SK territory it is not permitted to interfere with these rights within proceedings on an act which would not be criminal act pursuant to the SK law.

Section 550

Handing over of a thing

(1) Upon foreign authority's request, seizure of a thing may be executed and subsequent delivery of such thing to a foreign country.

Pursuant to the Criminal Code of the Slovak Republic, a thing means (with reference made to the provision of the Section 130, par. 2, Criminal Code of the Slovak Republic) also any non material information as well as any computer technology data.

note no 3:

With regard to the fact that the Slovak Republic has not ratified the Convention on Cybercrime so far, it also has not fully operating contact points (trained staff as well as necessary

equipment) for the purposes of the Convention on Cybercrime within the meaning of the Article 35 of the Convention.

Pursuant to the Act no. 211/2000, Coll., on free access to information, as amended (Act on Free Access to Information), every one has right of common access to the published information by means of telecommunication device, in particular by means of Internet, without showing any legal or other reason or interest for which the information is requested.

Article 32, letter b) of the Convention on Cybercrime corresponds with the Act no. 428/2002, Coll., on Protection of Personal Data as amended, in the cases where the person concerned gives consent to process his/her personal data.