



Cybercrime legislation – country profile

Hungary

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:	Hungary
Signature of Convention:	23th November 2001
Ratification/accession:	1st July 2004
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”	Art. 300/F of Hungarian Law no 4/1978 (Criminal Code) Art. 2 of Hungarian Law no 108/2001 (E-Commerce and IT) Art. 1 of Convention on cybercrime
<i>Chapter II – Measures to be taken at the national level</i>	
<i>Section 1 – Substantive criminal law</i>	
Article 2 – Illegal access	Art. 300/C and 300/E of Hungarian Law no 4/1978 (Criminal Code)
Article 3 – Illegal interception	Art. 300/C and 300/E of Hungarian Law no 4/1978 (Criminal Code)
Article 4 – Data interference	Art. 300/C and 300/E of Hungarian Law no 4/1978 (Criminal Code)
Article 5 – System interference	Art. 300/C and 300/E of Hungarian Law no 4/1978 (Criminal Code)
Article 6 – Misuse of devices	Art. 300/C and 300/E of Hungarian Law no 4/1978 (Criminal Code)
Article 7 – Computer-related forgery	Art. 300/C and 300/E of Hungarian Law no 4/1978 (Criminal Code)
Article 8 – Computer-	Art. 300/C and 300/E of Hungarian Law no 4/1978 (Criminal Code)

related fraud	
Article 9 – Offences related to child pornography	Art. 204 of Hungarian Law no 4/1978 (Criminal Code)
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	Art. 329/A-329/C of Hungarian Law no 4/1978 (Criminal Code)
Article 11 – Attempt and aiding or abetting	Art. 18 of Hungarian Law no 19/1998 (Criminal Procedure Law)
Article 12 – Corporate liability	Art. 7 of Hungarian Law no 108/2001 (E-Commerce and IT) Hungarian Law no 100/2003 (Communication of Information Law)
Article 13 – Sanctions and measures	Art. 204, 300/C, 300/E, 329/A-329/C of Hungarian Law no 19/1998 (Criminal Code)
<i>Section 2 – Procedural law</i>	
Article 14 – Scope of procedural provisions	Hungarian Law no 19/1998 (Criminal Procedure Law)
Article 15 – Conditions and safeguards	Hungarian Law no 19/1998 (Criminal Procedure Law)
Article 16 – Expedited preservation of stored computer data	Art. 151 of Hungarian Law no 100/2003 (Communication of Information Law)
Article 17 – Expedited preservation and partial disclosure of traffic data	Art. 151 of Hungarian Law no 100/2003 (Communication of Information Law)
Article 18 – Production order	Art. 151 of Hungarian Law no 100/2003 (Communication of Information Law)
Article 19 – Search and seizure of stored computer data	Art. 151 of Hungarian Law no 100/2003 (Communication of Information Law) Art. 151 of Hungarian Law no 19/1998 (Criminal Procedure Law)
Article 20 – Real-time collection of traffic data	Art. 151 of Hungarian Law no 100/2003 (Communication of Information Law)
Article 21 – Interception of content data	Art. 151 of Hungarian Law no 100/2003 (Communication of Information Law)
<i>Section 3 – Jurisdiction</i>	
Article 22 – Jurisdiction	Art. 3-5 of Hungarian Law no 4/1978 (Criminal Code)
<i>Chapter III – International co-operation</i>	
Article 24 – Extradition	Art. 3 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 25 – General principles relating to mutual assistance	Art. 36 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 26 – Spontaneous information	Art. 50 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 27 – Procedures pertaining to mutual	Art. 8 of Hungarian Law no 54/2002 (International Co-operation with Criminal Authorities in criminal matters)

assistance requests in the absence of applicable international agreements	
Article 28 – Confidentiality and limitation on use	Art. 50 and 66 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 29 – Expedited preservation of stored computer data	Art. 43 and 50 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 30 – Expedited disclosure of preserved traffic data	Art. 43 and 50 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 31 – Mutual assistance regarding accessing of stored computer data	Art. 43 and 50 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 32 – Trans-border access to stored computer data with consent or where publicly available	Art. 43 and 50 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 33 – Mutual assistance in the real-time collection of traffic data	Art. 43 and 50 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 34 – Mutual assistance regarding the interception of content data	Art. 43 and 50 of Hungarian Law no 130/2003 (Co-operation with European Union member states in criminal matters)
Article 35 – 24/7 Network	Art. 35 of Convention on cybercrime
Article 42 – Reservations	<p>Declaration contained in the instrument of ratification deposited on 4 December 2003 - Or. Engl.</p> <p>In accordance with Article 27, paragraph 9, sub-paragraph e, the Republic of Hungary informs that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority, due to practical reasons. Period covered: 1/7/2004 - The preceding statement concerns Article(s) : 27</p> <p>Reservation contained in the instrument of ratification deposited on 4 December 2003 - Or. Engl.</p> <p>In accordance with Article 9, paragraph 4, the Republic of Hungary reserves the right not to apply Article 9, paragraph 2, sub-paragraph b. Period covered: 1/7/2004 - The preceding statement concerns Article(s) : 9</p> <p>Declaration contained in the instrument of ratification deposited on 4 December 2003 - Or. Engl.</p> <p>In accordance with Article 24, paragraph 7, sub-paragraph a, of the Convention, the Republic of Hungary communicates that the Ministry of Justice is responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. The National Central Bureau of Interpol is only responsible for making or receiving requests for provisional arrest. Period covered: 1/7/2004 - The preceding statement concerns Article(s) : 24</p> <p>Declaration contained in the instrument of ratification deposited on 4 December 2003 - Or. Engl.</p> <p>In accordance with Article 27, paragraph 2, sub-paragraphs a and c, the</p>

	<p>Republic of Hungary communicates that, regarding requests delivered before starting the criminal procedure, the designated central authority is:</p> <p>The Hungarian National Police International Implementing Co-operation Centre Budapest, Teve u. 4-6 1139 – Hungary</p> <p>Regarding requests delivered after starting the criminal procedure, the designated central authority is:</p> <p>The General Prosecutor's Office of the Republic of Hungary Budapest, Markó u. 4-6 1055 - Hungary</p> <p>Period covered: 1/7/2004 - The preceding statement concerns Article(s) : 27</p> <p>Declaration contained in the instrument of ratification deposited on 4 December 2003 - Or. Engl.</p> <p>In accordance with Article 35, the Republic of Hungary communicates that the designated point of contact available on a twenty-four hour, seven-day-a-week basis is the Hungarian National Police International Implementing Co-operation Centre.</p> <p>Period covered: 1/7/2004 - The preceding statement concerns Article(s) : 35</p>
--	--

Appendix: **Solutions in national legislation.**

Act IV of 1978 on the Criminal Code

Territorial and Personal Scope

Section 3

(1) Hungarian law shall be applied to crimes committed in Hungary, as well as to acts committed by Hungarian citizens abroad, which are crimes in accordance with Hungarian law.

(2) The Hungarian law shall also be applied to criminal acts committed on board of Hungarian ships or Hungarian aircraft situated outside the borders of the Republic of Hungary.

Section 4

(1) Hungarian law shall also be applied to acts committed by non-Hungarian citizens abroad, if they are

a) criminal acts in accordance with Hungarian law and are also punishable in accordance with the law of the place of perpetration,

b) it is a criminal act against the state (Chapter X), excluding espionage against allied armed forces (Section 148),

regardless of whether it is punishable in accordance with the law of the country where committed,

c) crimes against humanity (Chapter XI) or any other crime, the prosecution of which is prescribed by an international treaty.

(2) Espionage (Section 148) against allied armed forces by a non-Hungarian citizen in a foreign country shall be punishable according to Hungarian penal law, provided that such offense is also punishable by the law of the country where committed.

(3) In the cases described in Subsections (1)-(2) the indictment shall be ordered by the Attorney General.

Diplomatic Exemption and other Exemption Based on International Law

Section 5

The criminal indictment of persons enjoying diplomatic immunity and other immunity based on international law shall be governed by international treaties, and failing this, by international practice. In the issue of international practice, the declaration made by the Minister of Justice shall be governing.

Extreme Necessity

Section 30

(1) The person who rescues his own person or goods or the person or goods of other people from a direct danger otherwise not preventable, or acts so in the defence of the public interest, shall not be punishable, provided that the occurrence of the danger is not imputable to him and his act causes a smaller injury than that for the prevention of which he made efforts.

(2) That person is not punishable either, who causes an injury of the same or greater extent than the one for the prevention of which he made efforts, because he is unable to recognize the magnitude of the injury due to fright or justifiable excitement.

(3) The punishment may be mitigated without limitation, if fright or justifiable excitement restricts the perpetrator in the recognition of the magnitude of the injury.

(4) No emergency may be established to the benefit of the person, whose professional duty is the undertaking of exposure to danger.

Criminal Conduct for Breaching Computer Systems and Computer Data

Section 300/C

(1) Any person who gains unauthorized entry to a computer system or network by compromising integrity of the computer protection system or device, or overrides or infringes his misdemeanor punishable by imprisonment not to exceed one year, work in community service.

(2) Any person who

a) without permission alters, damages or deletes data stored, processed or transmitted network or denies access to the legitimate users,

b) without permission adds, transmits, alters, damages, deletes any data, or uses any other computer system or network is guilty of misdemeanor punishable by imprisonment not community service or a fine.

(3) Any person who, for financial gain or advantage,

- a) alters, damages or deletes data stored, processed or transmitted in a computer system to the legitimate users,
- b) adds, transmits, alters, damages, deletes data or uses any other means to disrupt use network is guilty of felony punishable by imprisonment not to exceed three years.

(4) The punishment for the criminal act defined in Subsection (3) shall be

- a) imprisonment between one to five years if it causes considerable damage,
- b) imprisonment between two to eight years if it causes substantial damage,
- c) imprisonment between five to ten years if it causes particularly substantial damage.

Compromising or Defrauding the Integrity of the Computer Protection System or Device

Section 300/E

(1) Any person who, for the commission of the criminal activities defined in Section 300/C,

- a) creates,
- b) obtains,
- c) distributes or trades, or otherwise makes available computer software, passwords, entry codes, or other data with which to gain access to a computer system or network is guilty of misdemeanor punishable by imprisonment not to exceed two years, work in community service or a fine.

(2) Any person who, for the commission of the criminal activities defined in Section 300/C, conveys his economic, technical and/or organizational expertise to another person for the creation of computer software, passwords, entry codes, or other data with which to gain access to a computer system or network shall be punished according to Subsection (1).

(3) In the case of Paragraph a) of Subsection (1), any person who confesses to the authorities his involvement in the creation of any computer software, password, entry code, or other data with which to gain access to a computer system or entire computer network before the authorities learned of such activities through their own efforts, and if the person surrenders such produced things to the authorities and assists in the efforts to identify the other persons involved, shall be exonerated from punishment.

Interpretative Provision

Section 300/F

For the purposes of Sections 300/C and 300/E, 'computer system' means a device or a collection of devices intended for the automatic processing, handling, storage and transmission of data.

Infringement of Copyright and Certain Rights Related to Copyright

Section 329/A

(1) A person who infringes a right of the author of a literary, scientific or artistic creation attached to such work, a right of a performing artist attached to his performance, a right of a producer of a sound recording attached to his sound recording, a right of a radio or television organization attached to its program, or a right of the maker of motion picture or database attached to such work, for the purpose of financial gain or advantage and/or thereby causing financial injury, is guilty of a misdemeanor punishable by imprisonment not to exceed two years, work in community service or a fine.

(2) The punishment shall be imprisonment not exceeding three years for a felony, if the infringement of copyright or certain rights related to copyright

- a) causes substantial financial injury,
- b) is committed in a pattern of criminal profiteering.

(3) The punishment shall be

- a) imprisonment not exceeding five years, if the infringement of copyright or certain rights related to copyright results in particularly considerable financial injury,
- b) imprisonment between two to eight years, if the infringement of copyright or certain rights related to copyright results in particularly substantial financial injury.

(4) Any person who commits an infringement of copyright or certain rights related to copyright by negligence is guilty of misdemeanor punishable by imprisonment not to exceed one year, work in community service, or a fine.

Compromising or Defrauding the Integrity of Technological Measures for the Protection of Copyright and Certain Rights Related to Copyright

Section 329/B.

(1) Any person who

- a) manufactures or fabricates,
- b) supplies, distributes or deals

with any instrument, product, equipment and/or accessory for compromising the technological measures defined in the Act on Copyright instituted for the protection of copyright and certain

rights related to copyright is guilty of a misdemeanor punishable by imprisonment not to exceed two years, work in community service, or a fine.

(2) Any person who conveys economic, technical and/or organizational expertise to another person for the purpose of and as necessary for the defrauding of technological measures instituted for the protection of copyright and certain rights related to copyright shall be punished according to Subsection (1) above.

(3) The punishment shall be imprisonment not exceeding three years for a felony, if the act of defrauding the technological measures instituted for the protection of copyright and certain rights related to copyright is committed in a pattern of criminal profiteering.

(4) A person implicated in the offense described in Paragraph *a*) of Subsection (1) above shall not be punished if he voluntarily confesses to the authorities his involvement in the manufacture or production of any instrument, product, equipment and/or accessory intended for compromising the technological measures instituted for the protection of copyright and certain rights related to copyright prior to the authorities gaining knowledge of such, and if he surrenders such manufactured and fabricated objects to the authorities, and if he provides information concerning any other individuals participating in manufacture or production.

Falsifying Data Related to Copyright Management

Section 329/C.

Any person who, for financial gain or advantage, unlawfully removes or falsifies any data or information - defined as such in the Act on Copyright - and published in connection with the use of a work or performance of another person that is protected by copyright or certain rights related to copyright, is guilty of a misdemeanor punishable by imprisonment not to exceed two years, work in community service, or a fine.