**A MAGYAR KÖZTÁRSASÁG**
**KORMÁNYA**

**T/10850. számú**
**törvényjavaslat**

# az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai bűnözésről szóló Egyezményének kihirdetéséről

**Előadó:**

**Dr. Bárándy Péter**
**igazságügy-miniszter**

**Budapest, 2004. július**

**2004. évi … törvény**
**az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai bűnözésről szóló Egyezményének kihirdetéséről**

**1. §**

Az Országgyűlés az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai bűnözésről szóló Egyezményét (a továbbiakban: Egyezmény) e törvénnyel kihirdeti.

(A Magyar Köztársaság megerősítésről szóló okiratának letétbe helyezése az Európa Tanács Főtitkáránál 2003. december 4-én megtörtént; az Egyezmény – 36. Cikkének 3. bekezdése értelmében – a Magyar Köztársaság vonatkozásában 2004. július 1-jén lép hatályba.)

**2. §**

Az Egyezmény hiteles angol nyelvű szövege és annak hivatalos magyar nyelvű fordítása a következő:

„**Convention on cybercrime**

**Preamble**

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in 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 treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring

rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

## Chapter I – Use of terms

### Article 1 – Definitions

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.

#### 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.

#### 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.

#### 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.

#### 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 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.

**Article 8 – Computer-related fraud**

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.

*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 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.

*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 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.

**Article 13 – Sanctions and measures**

1. Each Party shall adopt such legislative and other measures as may be 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**

*Title 1 – Common provisions*

**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.

*Title 2 – Expedited preservation of stored computer data*

**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 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.

**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.

*Title 3 – Production order*

**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.

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.

*Title 4 – Search and seizure of stored computer data*

**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, 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.

*Title 5 – Real-time collection of computer data*

**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 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.

**Article 21 – Interception of content data**

1. Each Party shall adopt such legislative and other measures as may be 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.

**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.

5. 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.

## Chapter III – International co-operation

### Section 1 – General principles

*Title 1 – General principles relating to international co-operation*

#### Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes 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.

*Title 2 – Principles relating to extradition*

#### 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 that the details held on the register are correct at all times.

*Title 3 – General principles relating to mutual assistance*

**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 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 provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

*Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements*

**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, 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 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.

**Section 2 – Specific provisions**

*Title 1 – Mutual assistance regarding provisional measures*

**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.

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.

7. 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 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.

*Title 2 – Mutual assistance regarding investigative powers*

**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.

**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.

**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 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.

*Title 3 – 24/7 Network*

**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.

## Chapter IV – Final provisions

### Article 36 – Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

**Article 37 – Accession to the Convention**

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

**Article 38 – Territorial application**

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

**Article 39 – Effects of the Convention**

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

**Article 40 – Declarations**

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 possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

**Article 41 – Federal clause**

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

**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.

**Article 43 – Status and withdrawal of reservations**

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

**Article 44 – Amendments**

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

**Article 45 – Settlement of disputes**

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

**Article 46 – Consultations of the Parties**

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a) the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b) the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c) consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

**Article 47 – Denunciation**

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

**Article 48 – Notification**

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a) any signature;

b) the deposit of any instrument of ratification, acceptance, approval or accession;

c) any date of entry into force of this Convention in accordance with Articles 36 and 37;

d) any declaration made under Article 40 or reservation made in accordance with Article 42;

e) any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.”

**„Számítástechnikai bűnözésről szóló Egyezmény**

**Preambulum**

Az Európa Tanács tagállamai és a többi aláíró állam,

Figyelembe véve, hogy az Európa Tanács célja a tagjai közötti szorosabb egység megteremtése;

Felismerve a jelen Egyezményt aláíró többi Állammal való együttműködés erősítésének fontosságát;

Meggyőződve egy olyan közös büntetőjogi politika kialakításának szükségességéről, melynek elsődleges célja - többek között megfelelő jogszabályok elfogadásával és a nemzetközi együttműködés elősegítésével - a társadalom védelme a számítástechnikai bűnözéssel szemben;

Tudatában a számítástechnikai hálózatok folyamatos globalizációja, digitalizációja, konvergenciája által előidézett mélyreható változásoknak;

Törődve azzal a veszéllyel, hogy a számítástechnikai hálózatok és az elektronikai információk bűncselekmények elkövetésére is felhasználhatók, és a bűncselekményekkel összefüggő bizonyítékok számítástechnikai hálózatok útján tárolhatók és továbbíthatók;

Felismerve az Államok és a magánszektor közötti együttműködés szükségességét a számítástechnikai bűnözés elleni harcban, továbbá az információs technológiák használatához és fejlesztéséhez kapcsolódó törvényes érdekek védelmének szükségességét;

Elfogadva, hogy a számítástechnikai bűnözés elleni hatékony küzdelem széles körű, gyors és jól működő nemzetközi együttműködést követel meg a büntető ügyek területén;

Meggyőződve a jelen Egyezmény szükségességéről a számítástechnikai rendszerek, hálózatok és adatok hozzáférhetősége, sértetlensége és titkossága elleni cselekmények, valamint az ilyen rendszerek, hálózatok és adatok visszaélésszerű használatának megelőzésében, a jelen Egyezményben meghatározottaknak megfelelően büntetendővé nyilvánítva ezeket a cselekményeket, továbbá megalkotva a bűncselekményekkel szembeni hatékony fellépést lehetővé tevő, azok felderítését, nyomozását és üldözését mind nemzeti, mind nemzetközi szinten megkönnyítő megfelelő jogköröket, valamint elfogadva a gyors és megbízható nemzetközi együttműködést biztosító rendelkezéseket;

Szem előtt tartva a büntető jogalkalmazáshoz fűződő érdek és az alapvető emberi jogok védelme közötti megfelelő egyensúly biztosításának szükségességét, miként azt az Európa Tanács által 1950-ben elfogadott, Emberi Jogok és Alapvető Szabadságok Védelméről szóló Egyezmény, az Egyesült Nemzetek Szervezete által 1966-ban elfogadott, Polgári és Politikai Jogok Nemzetközi Egyezségokmánya, valamint az emberi jogokkal kapcsolatos más nemzetközi szerződések tartalmazzák, melyek megerősítik minden ember jogát a beavatkozásmentes véleménynyilvánításhoz, hasonlóan a véleménynyilvánítás szabadságához, ideértve azt a jogot, hogy mindenki szabadon, határokra tekintet nélkül kereshessen, megszerezhessen és közölhessen bármilyen tartalmú eszmét és információt, továbbá a magánélet tiszteletben tartásához fűződő jogot;

Figyelembe véve a személyes adatok védelméhez való jogot, melyet egyebek mellett a Személyes Adatok Automatikus Kezeléséről szóló Egyezményre tekintettel a Személyek Védelméről szóló 1981-ben elfogadott Európa Tanácsi Egyezmény tárgyal;

Figyelembe véve az Egyesült Nemzetek Szervezetének 1989-ben elfogadott Gyermekek Jogairól szóló Egyezményét, valamint a Nemzetközi Munkaügyi Szervezet 1999-ben elfogadott Gyermekmunka Legrosszabb Formáinak Betiltásáról és Felszámolására irányuló azonnali lépésekről szóló Egyezményt;

Figyelembe véve az Európa Tanács hatályos egyezményeit a büntetőjogi együttműködés területén, valamint az Európa Tanács tagállamai és más államok között megkötött hasonló tárgyú egyezményeket, kiemelve azt, hogy a jelen Egyezmény célja a hivatkozott egyezmények kiegészítése annak érdekében, hogy hatékonyabbá tegye a számítástechnikai rendszerek és adatok vonatkozásában elkövetetett bűncselekményekkel összefüggő nyomozást és büntetőeljárást, valamint lehetővé tegye a bűncselekmények elektronikus formában megjelenő bizonyítékainak összegyűjtését;

Üdvözölve a számítástechnikai bűnözés elleni küzdelem területén a nemzetközi együttműködés és megértés további fejlesztésére irányuló, a közelmúltban tett kezdeményezéseket, ideértve az Egyesült Nemzetek Szervezete, az OECD, az Európai Unió és a G-8-ak által meghozott intézkedéseket;

Emlékeztetve a Miniszteri Bizottság R (85) 10. számú Ajánlására a bűnügyi jogsegélyről szóló európai egyezmény alkalmazása a távközlési hálózatok lehallgatására vonatkozó megkeresések kapcsán, az R (88) 2. számú Ajánlására a szerzői és szomszédos jogokkal kapcsolatban elkövetett jogsértések elleni küzdelem érdekében hozandó intézkedésekről, az R (87) 15. számú Ajánlására a személyes adatok rendőrségi felhasználására vonatkozó szabályozásról, az R (95) 4. számú Ajánlására a személyes adatok védelméről a távközlési szolgáltatások terén, különös figyelemmel a távbeszélő szolgáltatásokra, valamint az R (89) 9. számú Ajánlására a számítógépekkel kapcsolatos bűncselekményekről, amely bizonyos számítástechnikai bűncselekmények meghatározása érdekében irányelveket tartalmaz a nemzeti jogalkotó részére, továbbá az R (95) 13. számú Ajánlására az információs technológiával összefüggő büntető eljárásjogi problémákról;

Tekintetbe véve az európai igazságügy-miniszterek 1997. június 10-11-i, XXI. Prágai Konferenciáján elfogadott 1. számú határozatot, mely a Miniszteri Bizottság számára javasolta, hogy támogassa a Büntetőjogi Problémákkal Foglalkozó Európai Bizottság (CDPC) számítástechnikai bűnözéssel kapcsolatos tevékenységét a nemzeti büntető jogalkotás közelítése és a számítástechnikai bűncselekményekkel szembeni hatékony nyomozati eszközök felhasználása érdekében, valamint az európai igazságügy-miniszterek 2000. június 8-9-i XXIII. Konferenciáján elfogadott 3. számú határozatot, mely az erőfeszítéseik folytatására ösztönözte a tárgyaló feleket annak érdekében, hogy megfelelő megoldásokat találjanak az Egyezményhez csatlakozó államok számának növelésére, és elismerve a számítástechnikai bűnözés elleni harc sajátos követelményeit figyelembe vevő, gyors és hatékony nemzetközi együttműködés eszközei megteremtésének szükségességét;

Ugyancsak figyelembe véve az új információs technológiák fejlődésével kapcsolatban az Európa Tanács értékein és normáin alapuló közös megoldások kidolgozására vonatkozó, az Európa Tanács állam-és kormányfőinek az 1997. október 10-11. között Strasbourgban megtartott Második Találkozójukon elfogadott akcióprogramot;

Megállapodtak az alábbiakban:

## ELSŐ RÉSZ

## ÉRTELMEZŐ RENDELKEZÉSEK

*1. Cikk*
*Meghatározások*

A jelen Egyezmény alkalmazása szempontjából:

a) „számítástechnikai rendszer” minden olyan eszköz, illetőleg egymással kapcsolatban lévő vagy összekötött eszközök összessége, amelyek, illetőleg amelyeknek egy vagy több eleme egy adott programnak megfelelően adatok automatikus feldolgozását végzi;

b) „számítástechnikai adat” tényeknek, információknak, illetőleg fogalmaknak minden olyan formában való megjelenése, mely számítástechnikai feldolgozásra alkalmas, ideértve azon programot is, mely valamely funkciónak a számítástechnikai rendszer által való végrehajtását biztosítja;

c) a „szolgáltató” jelentése:

i) minden olyan közjogi és magánjogi alany, mely a szolgáltatásait igénybe vevőknek biztosítja egy számítástechnikai rendszer általi érintkezés lehetőségét;

ii) minden más olyan alany, amely a kommunikációs szolgáltatásnak, illetőleg az azt igénybe vevők részére számítástechnikai adatokat feldolgoz vagy tárol;

d) „forgalmi adat” minden olyan, a számítástechnikai rendszeren átmenő és a számítástechnikai rendszer mint a kommunikációs lánc egyik eleme által létrehozott kommunikációra vonatkozó adat, mely jelzi a kommunikáció eredetét, rendeltetési helyét, útvonalát, idejét, napját, terjedelmét és időtartamát vagy a szolgáltatás típusát.

## MÁSODIK RÉSZ
## NEMZETI SZINTEN MEGHOZANDÓ INTÉZKEDÉSEK

### I. FEJEZET
### BÜNTETŐ ANYAGI JOG

#### *I. cím*
#### *Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények*

*2. Cikk*
*Jogosulatlan belépés*

Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a számítástechnikai rendszerbe vagy annak bármely részébe történő jogosulatlan és szándékos belépés. A Fél kikötheti, hogy a bűncselekményt a biztonsági intézkedések megsértésével vagy számítástechnikai adatok

megszerzésére irányuló, illetőleg más tisztességtelen céllal, avagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

*3. Cikk*
*Jogosulatlan kifürkészés*

Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a számítástechnikai rendszeren belüli, az abból származó, illetőleg a rendszerbe irányuló számítástechnikai adatok nem nyilvános továbbítása során technikai eszközök felhasználásával történő jogosulatlan és szándékos kifürkészése, ideértve az ilyen számítástechnikai adatokat továbbító, a számítástechnikai rendszerből származó elektromágneses sugárzást. A Fél kikötheti, hogy a bűncselekményt tisztességtelen céllal vagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

*4. Cikk*
*Számítástechnikai adat megsértése*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a számítástechnikai adatok jogosulatlan és szándékos megkárosítása, törlése, megrongálása, megváltoztatása vagy megsemmisítése.

2. A Fél fenntarthatja magának a jogot annak kikötésére, hogy az 1. bekezdésben meghatározott cselekmény eredményeként jelentős kár következzen be.

*5. Cikk*
*Számítástechnikai rendszer megsértése*

Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a számítástechnikai rendszer működésének számítástechnikai adatok bevitelével, továbbításával, megkárosításával, törlésével, megrongálásával, megváltoztatásával vagy megsemmisítésével való, jogosulatlan és szándékos, jelentős mértékű akadályozása.

*6. Cikk*
*Eszközökkel való visszaélés*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön az alábbi cselekmények jogosulatlan és szándékos elkövetése:

a) az előállítása, az értékesítése, a felhasználás céljából való megszerzése, az ország területére való behozatala, a forgalomba hozatala vagy a más módon történő hozzáférhetővé tétele:

i) elsődlegesen azon eszközöknek, ideértve a számítástechnikai programot, melyeket a 2-5. Cikkben meghatározott valamely bűncselekmény elkövetése érdekében hoztak létre vagy alakítottak át;

ii) egy számítógépes jelszónak, egy belépési kódnak, illetőleg hasonló, a számítástechnikai rendszerbe vagy annak bármely részébe való belépést lehetővé tevő számítástechnikai adatnak,

azzal a céllal, hogy azt a 2-5. Cikkekben foglalt valamely bűncselekmény elkövetésére használják fel; valamint

b) a fenti a) pont i és ii alpontjában meghatározott dolgoknak a birtoklása a 2-5. Cikkben foglalt valamely bűncselekmény elkövetésére való felhasználás érdekében. A Fél a belső jogában kikötheti, hogy a büntetőjogi felelősséget meghatározott számú dolog birtoklása alapozza meg.

2. Jelen Cikkben foglaltak nem alapozzák meg a büntetőjogi felelősséget abban az esetben, ha a jelen Cikk 1. bekezdésében foglalt előállításnak, értékesítésnek, felhasználás céljából való megszerzésnek, az ország területére való behozatalnak, forgalomba hozatalnak vagy más módon történő hozzáférhetővé tételnek nem célja a jelen Egyezmény 2-5. Cikkében meghatározott bűncselekmény elkövetése, mint például az engedélyezett kísérlet vagy valamely számítástechnikai rendszer védelme esetén.

3. Minden Szerződő Fél fenntarthatja magának azt a jogot, hogy nem alkalmazza a jelen Cikk 1. bekezdését, feltéve, hogy a fenntartás nem a jelen Cikk 1. bekezdése a) pontjának ii alpontjában meghatározott értékesítésre, forgalomba hozatalra vagy más módon történő hozzáférhetővé tételre vonatkozik.

## *II. cím*
## *Számítógéppel kapcsolatos bűncselekmények*

### *7. Cikk*
### *Számítógéppel kapcsolatos hamisítás*

Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a számítástechnikai adatoknak olyan, jogosulatlan és szándékos bevitele, megváltoztatása, törlése vagy megsemmisítése, melyek eredményeként nem valódi adatok jönnek létre abból a célból, hogy úgy lehessen azokat figyelembe venni vagy jogszerű célra felhasználni, mintha valódi adatok lennének, függetlenül attól a ténytől, hogy közvetlenül olvashatók vagy érthetők-e. A Fél kikötheti, hogy csalárd szándék vagy hasonló tartalmú tisztességtelen cél fennállása alapozza meg a büntetőjogi felelősséget.

### *8. Cikk*
### *Számítógéppel kapcsolatos csalás*

Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek

minősüljön a másnak jogosulatlanul és szándékosan történő vagyoni károkozás, amelyet

a) számítástechnikai adatok bármilyen bevitelével, megváltoztatásával, törlésével vagy megsemmisítésével;
b) a számítástechnikai rendszer működésébe való bármilyen beavatkozással,

anyagi haszon saját vagy más részére történő jogosulatlan megszerzésének céljából követnek el.

## *III. cím*
## *Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények*

### *9. Cikk*
### *Gyermek-pornográfiával kapcsolatos bűncselekmények*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljenek az alábbi cselekmények, amennyiben azokat jogosulatlanul és szándékosan követik el:

a) gyermek-pornográfia készítése számítástechnikai rendszer útján történő forgalomba hozatal céljából;
b) gyermek-pornográfia felajánlása vagy hozzáférhetővé tétele számítástechnikai rendszer útján;
c) gyermek-pornográfia továbbítása vagy forgalomba hozatala számítástechnikai rendszer útján;
d) gyermek-pornográfiának saját vagy más részére számítástechnikai rendszer útján történő megszerzése;
e) gyermek-pornográfiának egy számítástechnikai rendszerben vagy egy számítástechnikai adattároló-egységen való birtoklása.

2. A jelen Cikk 1. bekezdése alkalmazásában „gyermek-pornográfia” fogalma alatt olyan pornográf termék értendő, mely vizuális úton ábrázol:

a) kifejezetten szexuális magatartást tanúsító kiskorú személyt;
b) kifejezetten szexuális magatartást tanúsító kiskorúnak tűnő személyt;
c) kifejezetten szexuális magatartást tanúsító kiskorú személyt megjelenítő valósághű képet.

3. A jelen Cikk 2. bekezdése tekintetében „kiskorú” mindazon személy, aki még nem töltötte be 18. életévét. A Fél alacsonyabb korhatárt is meghatározhat, amely azonban nem lehet kevesebb a 16. életévnél.

4. Minden Szerződő Fél fenntarthatja magának azt a jogot, hogy részben vagy egészben nem alkalmazza a jelen Cikk 1. bekezdésének d) és e) pontját, valamint 2. bekezdésének b) és c) pontját.

## *IV. cím*
## *Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények*

*10. Cikk*
*Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a Fél joga szerint az Irodalmi és Művészeti Művek Védelméről szóló Berni Uniós Egyezményben és az azt felülvizsgáló 1971. június 24-én megkötött Párizsi Egyezményben, a Szellemi Tulajdonjogok Kereskedelmi Vonatkozásairól szóló Egyezményben, a Szellemi Tulajdon Világszervezete Szerzői Jogi Szerződésében foglalt és a Fél által elfogadott kötelezettségeknek megfelelően meghatározott szerzői jogok - kivéve a fenti egyezményekben megállapított bármely személyhez fűződő jogok - megsértése, amennyiben azt szándékosan, kereskedelmi méretekben és számítástechnikai rendszer útján követik el.

2. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a Fél joga szerint az Előadóművészek, a Hangfelvétel-előállítók és a Műsorsugárzó Szervezetek Védelméről szóló Római Egyezményben, a Szellemi Tulajdonjogok Kereskedelmi Vonatkozásairól szóló Egyezményben, a Szellemi Tulajdon Világszervezetének az előadásokról és a hangfelvételekről szóló szerződésében foglalt és a Fél által elfogadott kötelezettségeknek megfelelően meghatározott szomszédos jogok - kivéve a fenti egyezményekben megállapított bármely személyhez fűződő jogok - megsértése, amennyiben azt szándékosan, kereskedelmi méretekben és számítástechnikai rendszer útján követik el.

3. A Fél fenntarthatja magának azt a jogot, hogy egy szűk körben a jelen Cikk 1. és 2. bekezdésében foglaltak vonatkozásában eltekint a büntetőjogi felelősség megállapításától feltéve, hogy más hatékony jogorvoslati lehetőségek állnak rendelkezésre, valamint, hogy ez a fenntartás nem ellentétes az 1. és 2. bekezdésekben hivatkozott nemzetközi szerződések alapján a Felet terhelő kötelezettségekkel.

## *V. cím*
## *Egyéb felelősségi és büntetési formák*

*11. Cikk*
*Kísérlet és bűnsegély vagy felbujtás*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a jelen Egyezmény 2-10. Cikkeiben meghatározott bűncselekmény elkövetéséhez kapcsolódó, a bűncselekmény elkövetése érdekében szándékosan megvalósított bűnsegédi bűnrészesség vagy felbujtás.

2. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a jelen Egyezmény 3-5., 7., 8. Cikkében, valamint a 9. Cikk 1. bekezdésének a) és c) pontjában meghatározott bűncselekmények elkövetésének szándékos kísérlete.

3. Minden Szerződő Fél fenntarthatja magának azt a jogot, hogy a jelen Cikk 2. bekezdését részben vagy egészben nem alkalmazza.

*12. Cikk*
*Jogi személyek felelőssége*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy a jelen Egyezményben foglalt bűncselekményekkel kapcsolatban a jogi személyek felelősségre vonhatók legyenek, ha azt olyan természetes személy követi el a jogis személy javára, akár a saját, akár a jogi személy egyik szervének tagjaként eljárva, aki a jogi személyen belül vezető jogkörrel rendelkezik és mely jogkör alapja

a) a jogi személy képviseletének joga;
b) a jogi személy nevében döntések meghozatalának joga;
c) a jogi személyen belüli ellenőrzés joga.

2. Az 1. bekezdésben már meghatározott eseten túl minden Szerződő Fél megteszi azon szükséges intézkedéseket, melyek biztosítják, hogy a jogi személy felelősségre vonható legyen abban az esetben is, ha az 1. bekezdésben említett természetes személy részéről gyakorolt felügyelet vagy ellenőrzés hiánya teszi lehetővé, hogy a felügyelete alá tartozó természetes személy a jogi személy javára elkövesse a jelen Egyezményben meghatározott bűncselekményeket.

3. A Fél jogi alapelveivel összhangban a jogi személy felelőssége lehet büntetőjogi, polgári jogi vagy közigazgatási jogi.

4. A jogi személy felelősségének megállapítása nem zárja ki a bűncselekményt elkövető természetes személy büntetőjogi felelősségének megállapítását.

*13. Cikk*
*Büntetések és intézkedések*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy a 2-11. Cikkben meghatározott bűncselekmények miatt arányos, hatékony, és visszatartó erejű büntetéseket lehessen alkalmazni, ideértve a szabadságelvonó büntetéseket is.

2. Minden Szerződő Fél biztosítja, hogy arányos, hatékony és visszatartó erejű büntetőjogi, illetőleg nem büntetőjogi szankciókkal vagy intézkedésekkel, ideértve a pénzügyi szankciókat is, lehessen sújtani azokat a jogi személyeket, amelyek felelősségét a 12. Cikk alkalmazásával állapították meg.

## II. FEJEZET
## BÜNTETŐ ELJÁRÁSI JOG

### *I. Cím*
### *Általános rendelkezések*

*14. Cikk*
*Az eljárásjogi rendelkezések alkalmazási köre*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek meghatározott bűnügyi nyomozás vagy büntetőeljárás érdekében a jelen fejezetben szereplő jogkörök és eljárások megteremtéséhez szükségesek.

2. A 21. Cikkben foglalt ellenkező rendelkezés hiányában minden Szerződő Fél alkalmazza a jelen címben meghatározott jogköröket és eljárásokat:

a) a jelen Egyezmény 2-11. Cikkeiben meghatározott bűncselekményekkel kapcsolatban;
b) a számítástechnikai rendszer útján elkövetett más bűncselekményekkel kapcsolatban és
c) a bűncselekménnyel összefüggő elektronikus bizonyítékok összegyűjtésével kapcsolatban.

3. a) Minden Szerződő Fél fenntarthatja magának azt a jogot, hogy a 20. Cikkben meghatározott intézkedéseket csak a fenntartásban meghatározott bűncselekményekkel vagy bűncselekmény kategóriákkal összefüggésben alkalmazza, feltéve, hogy ezen bűncselekmények vagy bűncselekmény kategóriák köre nem szűkebb azon bűncselekményekénél, melyekre a 21. Cikkben meghatározott intézkedéseket alkalmazza. Minden Szerződő Fél törekszik arra, hogy korlátozza ezt a fenntartást oly módon, hogy lehetővé tegye a 20. Cikkben meghatározott intézkedések minél szélesebb körű alkalmazását.

b) Ha a Fél, a jelen Egyezmény elfogadásakor hatályban lévő jogi szabályozásában lévő korlátozások miatt nem alkalmazhatja a 20. és 21. Cikkben foglalt intézkedéseket a szolgáltató számítástechnikai rendszerén belül továbbított kommunikációra, mely rendszert

i) zárt felhasználói csoport érdekében működtetnek, és

ii) nem vesz igénybe közérdekű távközlő hálózatot, illetőleg nem kapcsolódik más magán vagy közérdekű számítástechnikai rendszerhez,

akkor a Fél fenntarthatja magának azt a jogot, hogy nem alkalmazza ezeket az intézkedéseket az említett kommunikációval összefüggésben. Minden Szerződő Fél törekszik arra, hogy korlátozza ezt a fenntartást oly módon, hogy lehetővé tegye a 20. és 21. Cikkben meghatározott intézkedések minél szélesebb körű alkalmazását.

*15. Cikk*
*Garanciák és biztosítékok*

1. Minden Szerződő Fél biztosítja, hogy a jelen fejezetben meghatározott jogkörök és eljárások megteremtése, bevezetése és alkalmazása során figyelembe veszi a belső jogában meghatározott biztosítékokat és garanciákat, melyek érvényre juttatják az arányosság elvét és lehetővé teszik az emberi jogok és szabadságok

megfelelő védelmét, különösen azokét a jogokét, melyeket az Európa Tanácsnak az Emberi Jogok és Alapvető Szabadságok Védelméről szóló Egyezményében (1950) és az Egyesült Nemzetek Szervezetének a Polgári és Politikai Jogok Nemzetközi Egyezségokmányában (1966), valamint más, az emberi jogokkal kapcsolatos nemzetközi szerződésben meghatározott és a Fél által vállalt kötelezettségekkel összefüggésben iktatott be jogrendszerébe.

2. Ha ez az érintett jogkör vagy eljárás természete miatt indokoltnak tűnik, a biztosítékok és garanciák többek között az eljárás vagy a jogkör alkalmazási időtartamát, alkalmazási köre korlátozását, illetőleg alkalmazását alátámasztó indokok meglétét, valamint bírói vagy más független szervezet általi felülvizsgálatát is jelenthetik.

3. Amennyiben az a közérdekkel, különösen az igazságszolgáltatás megfelelő működtetésével összeegyeztethető, minden Szerződő Fél megvizsgálja a jelen fejezetben meghatározott jogköröknek és eljárásoknak a harmadik személy jogaira, jogos érdekeire és felelősségére gyakorolt hatását.

## *II. Cím*
## *Tárolt számítástechnikai adat* gyors *megőrzése*

### *16. Cikk*
### *Tárolt számítástechnikai adat* gyors *megőrzése*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy lehetővé tegye az illetékes hatóságainak a számítástechnikai rendszerben tárolt meghatározott számítástechnikai adatok, ideértve a forgalmi adatok gyors megőrzésének elrendelését vagy más módon történő kikényszerítését, különösen ha alappal feltételezhető, hogy az érintett adatokat a módosulás vagy a megsemmisülés veszélyezteti.

2. Amennyiben a Fél az 1. bekezdés alkalmazása érdekében elrendeli, hogy egy adott személy őrizze meg a birtokában vagy az ellenőrzése alatt lévő meghatározott tárolt adatokat, akkor a Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy kötelezhesse ezt a személyt a fenti adatoknak addig az időtartamig, de legfeljebb kilencven napig történő megőrzésére és épségének megóvására, mely időtartam a hatóság részére az adatok átadására kötelezéshez szükséges. A Fél az intézkedés ismételt elrendelését is lehetővé teheti.

3. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy kötelezze az adatokat őrző személyt vagy más, az adatok megőrzésére köteles személyt a fenti eljárás lefolytatásának a belső jog által meghatározott időtartamig történő titokban tartására.

4. A jelen Cikkben meghatározott jogköröket és eljárásokat alá kell rendelni a 14. és 15. Cikkben foglalt rendelkezéseknek.

### *17. Cikk*
### *Forgalmi adat gyors megőrzése és részbeni átadása*

1. A forgalmi adatok 16. Cikk szerinti megőrzése érdekében, minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy:

a) biztosítsa a forgalmi adatoknak a gyors megőrzését, függetlenül attól, hogy egy vagy több szolgáltató vett részt a fenti kommunikáció továbbításában; és

b) biztosítsa megfelelő számú forgalmi adatnak a Fél illetékes hatósága vagy e hatóság által kijelölt személy részére történő gyors átadását a kommunikáció továbbítására igénybe vett útvonal és a szolgáltató azonosítása érdekében.

2. A jelen Cikkben meghatározott jogköröket és eljárásokat alá kell rendelni a 14. és 15. Cikkben foglalt rendelkezéseknek.

## *III. Cím*
## *Közlésre kötelezés*

### *18. Cikk*
### *Közlésre kötelezés*

1. Minden Szerződő Fél megteszi a szükséges jogalkotási és egyéb intézkedéseket, hogy az illetékes hatóságai kötelezhessék:

a) a területén tartózkodó személyt a birtokában vagy az ellenőrzése alatt lévő számítástechnikai rendszerben vagy számítástechnikai adattároló-egységen tárolt meghatározott számítástechnikai adatok közlésére; és

b) a területén szolgáltatást nyújtó szolgáltatót a birtokában vagy az ellenőrzése alatt lévő, az előfizetőre vonatkozó és a szolgáltatást érintő adatok közlésére.

2. A jelen Cikkben meghatározott jogköröket és eljárásokat alá kell rendelni a 14. és 15. Cikkben foglalt rendelkezéseknek.

3. Jelen Cikk alkalmazásában az „előfizetőre vonatkozó adat” bármely olyan számítástechnikai adat formájában vagy más formában megjelenő, szolgáltató által birtokolt, a szolgáltatásaira előfizetőkkel kapcsolatos, a tartalomra vonatkozó vagy a forgalmi adatoktól eltérő információ, mely lehetővé teszi, hogy megállapítsák:

a) az igénybe vett kommunikációs szolgáltatás típusát, az erre vonatkozóan tett technikai intézkedéseket, valamint a szolgáltatás időszakát;

b) az előfizető személyazonosságát, postai vagy földrajzi címét, telefonszámát vagy más elérhetőségét, a fizetésre és a számlázásra vonatkozó adatokat, melyek szolgáltatási szerződés vagy megállapodás alapján állnak a szolgáltató rendelkezésére;

c) minden más, a kommunikációs berendezés helyére vonatkozó, szolgáltatási szerződés vagy megállapodás alapján a szolgáltató rendelkezésére álló információt.

## *IV. Cím*
## *Tárolt számítástechnikai adat átvizsgálása és lefoglalása*

### *19. Cikk*
### *Tárolt számítástechnikai adat átvizsgálása és lefoglalása*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy feljogosítsa az illetékes hatóságait a területükön található:

a) számítástechnikai rendszer vagy annak egy része és az abban tárolt számítástechnikai adatok és

b) a számítástechnikai adatok tárolását lehetővé tevő számítástechnikai adattároló-egység

átvizsgálására vagy ahhoz más módon történő hozzáférésre.

2. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek annak biztosításához szükségesek, hogy amikor a hatóságai az 1. bekezdés a) pontjában foglalt intézkedések alkalmazásával átvizsgálnak vagy más hasonló módon hozzáférnek egy meghatározott számítástechnikai rendszerhez vagy annak egy részéhez, és alappal feltételezhetik, hogy a keresett adatokat a Fél területén található más számítástechnikai rendszerben vagy annak egy részében tárolják, és ezek az adatok a kiinduló rendszerből jogszerűen elérhetőek vagy a kiinduló rendszer számára hozzáférhetőek, akkor az említett hatóságok haladéktalanul kiterjeszthessék az átvizsgálást vagy a más hasonló módon történő hozzáférést a másik rendszerre is.

3. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy feljogosítsa az illetékes hatóságait azon számítástechnikai adatok lefoglalására vagy más hasonló módon való biztosítására, melyekhez az 1. vagy a 2. bekezdésben foglaltak alkalmazásával fértek hozzá. Ezek az intézkedések a következő jogosultságokat foglalják magukba:

a) számítástechnikai rendszer vagy annak része, illetőleg számítástechnikai adattároló-egység lefoglalása vagy más hasonló módon történő biztosítása;

b) számítástechnikai adatról másolat készítése és annak megőrzése;

c) a szükséges tárolt számítástechnikai adatok épségének megóvása; és

d) az átvizsgált számítástechnikai rendszer fenti számítástechnikai adatainak hozzáférhetetlenné tétele vagy eltávolítása.

4. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek illetékes hatóságai feljogosításához szükségesek, hogy azok kötelezhessék a számítástechnikai rendszer működését vagy a számítástechnikai adatok védelme érdekében alkalmazott intézkedéseket ismerő személyeket - amennyiben indokolt - mindazon szükséges tájékoztatás megadására, amely lehetővé teszi az 1. és 2. bekezdésben foglalt intézkedések alkalmazását.

5. A jelen Cikkben meghatározott jogköröket és eljárásokat alá kell rendelni a 14. és 15. Cikkben foglalt rendelkezéseknek.

## *V. Cím*
## *Számítástechnikai adatok valós idejű összegyűjtése*

### *20. Cikk*
### *Forgalmi adatok valós idejű összegyűjtése*

1. Minden Szerződő Fél megteszi azon szükséges jogalkotási és egyéb intézkedéseket, melyekkel az illetékes hatóságait feljogosítja arra, hogy

a) a Szerződő Fél területén található technikai eszközök felhasználásával valós időben összegyűjtsék vagy rögzítsék a számítástechnikai rendszer útján a területükön továbbított meghatározott kommunikációhoz kapcsolódó forgalmi adatokat; és

b) kötelezzék a szolgáltatókat, hogy a meglévő technikai teljesítőképességük körén belül:

i) a Szerződő Fél területén található technikai eszközök felhasználásával valós időben összegyűjtsék vagy rögzítsék a számítástechnikai rendszer útján a területükön továbbított meghatározott kommunikációhoz kapcsolódó forgalmi adatokat, vagy

ii) együttműködjenek és segítséget nyújtsanak az illetékes hatóságoknak az ilyen adatok valós idejű összegyűjtésében vagy rögzítésében.

2. Amennyiben a Fél, belső jogának alapelveire tekintettel, nem fogadhatja el az 1. bekezdés a) pontjában foglalt rendelkezéseket, azok helyett megteheti azon jogalkotási és más intézkedéseket, melyek a területén továbbított meghatározott kommunikációkkal kapcsolatos forgalmi adatok valós idejű összegyűjtésének vagy rögzítésének - a területén található technikai eszközök alkalmazásával történő – biztosításához szükségesek.

3. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy kötelezze a szolgáltatókat a jelen Cikkben meghatározott jogkörök gyakorlásának, valamint azzal kapcsolatos egyéb információknak a titokban tartására.

4. A jelen Cikkben meghatározott jogköröket és eljárásokat alá kell rendelni a 14. és 15. Cikkben foglalt rendelkezéseknek.

*21. Cikk*
*Tartalomra vonatkozó adatok kifürkészése*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy a belső jogban meghatározott súlyos bűncselekményekkel összefüggésben feljogosítsa az illetékes hatóságait, hogy

a) a Szerződő Fél területén található technikai eszközök felhasználásával valós időben összegyűjtsék vagy rögzítsék a számítástechnikai rendszer útján a területükön továbbított meghatározott kommunikációk tartalmára vonatkozó adatokat; és

b) kötelezzék a szolgáltatókat, hogy a meglévő technikai teljesítőképességük körén belül:

i) a Szerződő Fél területén található technikai eszközök felhasználásával valós időben összegyűjtsék vagy rögzítsék a számítástechnikai rendszer útján a területükön továbbított meghatározott kommunikációk tartalmára vonatkozó adatokat, vagy

ii) együttműködjenek és segítséget nyújtsanak az illetékes hatóságoknak az ilyen adatok valós idejű összegyűjtésében vagy rögzítésében.

2. Amennyiben a Fél, belső jogának alapelveire tekintettel, nem fogadhatja el az 1. bekezdés a) pontjában foglalt rendelkezéseket, azok helyett megteheti azon jogalkotási és más intézkedéseket, amelyek a területén továbbított meghatározott kommunikációk tartalmára vonatkozó adatok valós idejű összegyűjtésének vagy rögzítésének - a területén található technikai eszközök alkalmazásával történő – biztosításához szükségesek.

3. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy kötelezze a szolgáltatókat a jelen Cikkben meghatározott jogkörök gyakorlásának, valamint azzal kapcsolatos egyéb információknak a titokban tartására.

4. A jelen Cikkben meghatározott jogköröket és eljárásokat alá kell rendelni a 14. és 15. Cikkben foglalt rendelkezéseknek.

## III. FEJEZET
## JOGHATÓSÁG

*22. Cikk*
*Joghatóság*

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy megállapítsa joghatóságát a jelen Egyezmény 2-11. Cikkében foglaltaknak megfelelően meghatározott bűncselekmények vonatkozásában, amennyiben a bűncselekményeket:

a) a területén; vagy

b) a Fél lobogóját viselő hajó fedélzetén; vagy

c) a Félnél lajstromozott repülőgép fedélzetén követték el; vagy

d) melyet állampolgára követett el, ha a bűncselekmény az elkövetés helyének joga szerint büntetendő, vagy ha a bűncselekmény nem tartozik egyetlen állam joghatósága alá sem.

2. Minden Szerződő Fél fenntarthatja magának azt a jogot, hogy az 1. bekezdés b-d pontjában foglalt joghatóságra vonatkozó szabályokat vagy azok bármely részét nem, vagy csak meghatározott esetben, illetve feltételek között alkalmazza.

3. Minden Szerződő Félnek meg kell tennie azokat az intézkedéseket, melyek ahhoz szükségesek, hogy megállapítsa joghatóságát a jelen Egyezmény 24. Cikkének 1. bekezdésében foglalt bűncselekmények vonatkozásában, ha a bűncselekmény feltételezett elkövetője a területén tartózkodik, és a kiadatási kérelem kizárólag az elkövető állampolgársága miatt nem teljesíthető a másik Fél részére.

4. Jelen Egyezmény nem zárja ki a Fél belső joga szerint meghatározott büntetőjogi joghatóságának gyakorlását.

5. Ha több Fél joghatósága is kiterjed a jelen Egyezményben meghatározott feltételezett bűncselekményre, akkor az érintett Felek, amennyiben az célszerűnek mutatkozik, tárgyalást folytatnak annak érdekében, hogy eldöntsék, hogy melyik az a Fél, aki megfelelőbben tudja lefolytatni az eljárást.

## HARMADIK RÉSZ
## NEMZETKÖZI EGYÜTTMŰKÖDÉS

### I. FEJEZET
### ALAPELVEK

#### *I. Cím*
#### *A nemzetközi együttműködésre vonatkozó alapelvek*

*23. Cikk*
*A nemzetközi együttműködésre vonatkozó alapelvek*

A Felek, a jelen részben foglalt rendelkezéseknek megfelelően, a büntetőjogi tárgyú nemzetközi együttműködésekre vonatkozó nemzetközi szerződéseket, valamint az egységes vagy kölcsönös jogi szabályozásukon alapuló megállapodásokat, továbbá a nemzeti jogaikat alkalmazva, a lehető legszélesebb körben együttműködnek a számítástechnikai rendszerekkel és adatokkal kapcsolatos bűncselekményekre vonatkozó nyomozások és eljárások során, illetőleg bármely bűncselekményre vonatkozó elektronikus bizonyítékok összegyűjtése érdekében.

#### *II. Cím*
#### *Kiadatásra vonatkozó alapelvek*

*24. Cikk*
*Kiadatás*

1. a) E Cikk rendelkezései kerülnek alkalmazásra a Felek közötti kiadatásnál a jelen Egyezmény 2-11. Cikkeinek megfelelően meghatározott bűncselekményekre, azzal a feltétellel, hogy azok mindkét érdekelt Fél jogszabályai szerint legalább egy év, vagy ennél súlyosabb szabadságvesztés büntetéssel büntetendőek legyenek.

b) Ha két vagy több Fél között alkalmazható, egységes vagy viszonossági jogszabályon alapuló megállapodás, illetve kiadatási szerződés - beleértve az Európai Kiadatási Egyezményt (STE n 24) – alapján más minimális büntetés kerül alkalmazásra, az ilyen megállapodásban vagy szerződésben meghatározott minimális büntetést kell alkalmazni.

2. A jelen Cikk 1. bekezdésében meghatározott bűncselekményeket úgy kell tekinteni, mint a kiadatás alapjául szolgáló olyan bűncselekményeket, amelyekre kiterjed a Felek között hatályban lévő két- vagy többoldalú kiadatási szerződés. A Felek kötelezettséget vállalnak arra, hogy ezeket a bűncselekményeket mint a kiadatás alapjául szolgáló bűncselekményeket beiktatják a közöttük megkötendő valamennyi két- vagy többoldalú kiadatási szerződésbe.

3. Ha a Fél szerződés meglététől teszi függővé a kiadatást, és olyan Fél intéz hozzá kiadatási kérelmet, amelyikkel nem kötött kiadatási szerződést, akkor a jelen Egyezményt a kiadatás jogi alapjaként veheti figyelembe a jelen Cikk 1. bekezdésében meghatározott bűncselekmények tekintetében.

4. A Felek, akik a kiadatást nem teszik szerződés meglététől függővé, a jelen Cikk 1. bekezdésében meghatározott bűncselekményeket a kiadatás alapjául szolgáló bűncselekményekként ismerik el.

5. A kiadatásnak a megkeresett Fél belső jogában vagy a hatályban lévő kiadatási szerződésekben meghatározott feltételeknek kell megfelelnie, ideértve azokat az okokat is, melyek alapján a megkeresett Fél megtagadhatja a kiadatási kérelem teljesítését.

6. Ha a jelen Cikk 1. bekezdésében említett bűncselekmények vonatkozásában kizárólag a kiadni kért személy állampolgársága alapján vagy azért tagadják meg a kiadatást, mert a megkeresett Fél saját joghatósága alá tartozónak ítéli a bűncselekményt, akkor a megkeresett Fél, a megkereső Fél kérelmére, az eljárás lefolytatása érdekében a saját, hatáskörrel rendelkező hatóságai elé terjeszti az ügyet, és megfelelő időn belül beszámol a megkereső Félnek az ügy kimeneteléről. Az említett hatóságok a nyomozás és az eljárás lefolytatása, valamint a döntés meghozatala során a megkeresett Félnek a hasonló jellegű bűncselekményekre irányadó szabályai szerint járnak el.

7. a) Az aláírás, illetve a megerősítő, elfogadó, jóváhagyó vagy csatlakozó okmány letétbe helyezése alkalmával mindegyik Fél közli az Európa Tanács Főtitkárával valamennyi azon hatóság nevét és címét, amelynek hatáskörébe tartozik

szerződés hiányában a kiadatási, illetve az ideiglenes kiadatási letartóztatásra irányuló kérelmek előterjesztése vagy fogadása.

b) Az Európa Tanács Főtitkára a Fél által kijelölt hatóságokról nyilvántartást hoz létre és napra készen vezet. Minden Szerződő Félnek folyamatosan biztosítania kell a nyilvántartásba foglalt adatok pontosságát.

## *III. Cím*
## *A jogsegély általános alapelvei*

### *25. Cikk*
### *A jogsegély általános alapelvei*

1. A Felek a lehető legszélesebb körben jogsegélyt nyújtanak egymásnak a számítástechnikai rendszerekkel és adatokkal kapcsolatos bűncselekményekre vonatkozó nyomozások és eljárások során, illetőleg bármely bűncselekményre vonatkozó elektronikus bizonyítékok összegyűjtése érdekében.

2. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy eleget tegyen a 27-35. Cikkben foglalt kötelezettségeknek.

3. Sürgős esetben minden Szerződő Fél előterjeszthet jogsegély kérelmeket és arra vonatkozó tájékoztatásokat gyors kommunikációs csatornákon keresztül – mint például az elektronikus levél vagy a fax, amennyiben ezek a csatornák biztosítják a közlés biztonságát és azonosíthatóságát (ide értve, amennyiben szükséges, a titkosítást is), és a megkeresett Fél kérelmére azok hivatalos úton is megerősíthetők. A megkeresett Fél átveszi a jogsegély kérelmeket, és gyors kommunikációs csatornákon keresztül válaszol azokra.

4. Amennyiben a jelen Rész Cikkei kifejezetten másként nem rendelkeznek, a jogsegélynek a megkeresett Fél belső jogában vagy az alkalmazandó jogsegély-szerződésekben meghatározott feltételeknek kell megfelelnie, ideértve azon indokokat is**,** melyek alapján a megkeresett Fél megtagadhatja az együttműködést. A megkeresett Fél nem tagadhatja meg a jogsegélyt kizárólag azon indok alapján, hogy a kérelem olyan, a 2-11. Cikkben meghatározott bűncselekménnyel kapcsolatos, melyet a megkeresett Fél pénzügyi bűncselekménynek tekint.

5. Ha a megkeresett Fél, jelen rész rendelkezéseinek megfelelően, jogosult arra, hogy a jogsegély teljesítését a cselekmény mindkét Fél részéről fennálló büntethetőségétől tegye függővé, akkor ezt a feltételt teljesítettnek kell tekinteni, ha a bűncselekmény alapjául szolgáló cselekmény, melyre a jogsegély iránti kérelem vonatkozik, a megkeresett Fél belső jogában bűncselekménynek minősül függetlenül attól, hogy a megkereső Fél ugyanabba a bűncselekményi kategóriába sorolja-e a cselekményt vagy ugyanazon elnevezéssel illeti-e.

### *26. Cikk*
### *Megkeresés nélküli tájékoztatás*

1. A Fél, belső joga által meghatározott keretek között és előzetes megkeresés hiányában is, közölheti egy másik Féllel a saját nyomozása során megszerzett információkat, amennyiben úgy ítéli meg, hogy ezzel segíthet a címzett Félnek a jelen Egyezménnyel összhangban meghatározott bűncselekményekre vonatkozó nyomozások vagy eljárások elrendelésében és megfelelő lefolytatásában, vagy amennyiben ezek az információk azt eredményezhetik, hogy a Fél a jelen részben foglalt együttműködés iránti kérelmet terjesszen elő.

2. Az információk átadása előtt az átadó Fél kérheti az információk titokban tartását, vagy azoknak meghatározott feltételekhez kötött felhasználását. Ha a címzett Fél nem tud eleget tenni a fenti kérelemnek, tájékoztatnia kell erről az átadó Felet, aki dönt arról, hogy az információkat mindezek ellenére átadja-e. Ha a címzett Fél a megszabott feltételek szerint elfogadja az információkat, akkor ezt követően a feltételek szerint kell eljárnia.

## *IV. Cím*
## *Jogsegélykérelemmel kapcsolatos eljárások hatályos nemzetközi megállapodások hiányában*

### *27. Cikk*
### *Jogsegélykérelemmel kapcsolatos eljárás hatályos nemzetközi megállapodások hiányában*

1. Jogsegélyszerződés vagy a megkereső Fél és a megkeresett Fél között hatályban lévő egységes vagy kölcsönös jogi szabályozásukon alapuló megállapodás hiányában jelen Cikk 2-9. bekezdéseiben foglalt rendelkezéseket kell alkalmazni. Jelen Cikk rendelkezéseit nem kell alkalmazni, amennyiben létezik hasonló jellegű jogi szabályozás vagy megállapodás, kivéve ha az érintett Felek azok helyett a jelen Cikkben foglalt rendelkezések részleges vagy teljes alkalmazása mellett döntöttek.

2. a) Minden Szerződő Fél kijelöl egy vagy több központi hatóságot, akik jogosultak lesznek a jogsegély kérelmek előterjesztésére, az azokra történő válaszadásra, azok teljesítésére vagy azoknak a teljesítés érdekében a hatáskörrel rendelkező hatóságokhoz történő megküldésére;

b) A központi hatóságok közvetlenül érintkeznek egymással;

c) Minden Szerződő Fél jelen Egyezmény aláírása vagy a megerősítő, elfogadó, jóváhagyó vagy csatlakozási okmányok letétbe helyezése alkalmával közli az Európa Tanács Főtitkárával a jelen bekezdésben foglaltak szerint kijelölt hatóságok nevét és címét;

d) Az Európa Tanács Főtitkára nyilvántartást hoz létre és napra készen vezet a Felek által kijelölt központi hatóságokról. Minden Szerződő Félnek folyamatosan biztosítania kell a nyilvántartásba foglalt adatok pontosságát.

3. A jelen Cikkben foglalt jogsegélykérelmeket a megkereső Fél által meghatározott eljárás szerint kell teljesíteni, kivéve ha az nem egyeztethető össze a megkeresett Fél jogi szabályozásával.

4. A 25. Cikk 4. bekezdésében foglalt megtagadási okokon felül, a megkeresett Fél az alábbi esetekben is megtagadhatja a jogsegélyt:

a) ha a kérelem olyan bűncselekményre vonatkozik, amelyet a megkeresett Fél politikai bűncselekménynek, vagy politikai bűncselekménnyel összefüggő cselekménynek tekint;
b) ha a megkeresett Fél úgy ítéli meg, hogy a kérelem teljesítése sértheti országa szuverenitását, biztonságát, közrendjét vagy más lényeges érdekeit.

5. A megkeresett Fél elhalaszthatja a kérelemben meghatározott intézkedések végrehajtását, ha úgy ítéli meg, hogy azok hátrányosan befolyásolják a hatóságai által folytatott nyomozást vagy eljárást.

6. Az együttműködés megtagadását vagy elhalasztását megelőzően a megkeresett Fél, miután az adott eset kapcsán egyeztetett a megkereső Féllel, megvizsgálja, hogy részben vagy az általa szükségesnek tartott feltételek betartása mellett tudja-e teljesíteni a jogsegélyt.

7. A megkeresett Fél haladéktalanul tájékoztatja a megkereső Felet a jogsegélykérelemmel kapcsolatos döntéséről. A megkeresett Fél köteles megindokolni a kérelem teljesítését megtagadó vagy elhalasztó döntését. A megkeresett Fél tájékoztatja a megkereső Felet a jogsegélykérelem teljesítését jelentősen késleltető vagy azt lehetetlenné tevő bármilyen körülményről.

8. A megkereső Fél kérheti, hogy a megkeresett Fél tartsa titokban mind a jelen Cikk alapján előterjesztett jogsegélykérelem tényét, mind annak tárgyát, kivéve amennyiben az a kérelem teljesítéséhez szükséges. Ha a megkeresett Fél nem tud eleget tenni a titkosítási kérelemnek, haladéktalanul tájékoztatnia kell erről a megkereső Felet, aki dönt arról, hogy kéri-e mindezek ellenére a jogsegélykérelem teljesítését.

9. a) Sürgős esetben a megkereső Fél igazságügyi hatóságai a jogsegélykérelmeket és az arra vonatkozó tájékoztatásokat közvetlenül a megkeresett Fél megfelelő igazságügyi hatóságaihoz intézhetik. Ebben az esetben a megkereső Fél központi hatóságai útján a másolatokat egyidejűleg megküldi a megkeresett Fél központi hatóságainak.

b) A jelen bekezdés szerint meghatározott tájékoztatásokat és jogsegélykérelmeket a Nemzetközi Bűnügyi Rendőrségi Szervezet (Interpol) útján is elő lehet terjeszteni.

c) Ha a kérelem vagy tájékoztatás a jelen bekezdés a) pontjában foglaltakon alapul és ha az a hatóság, amelyhez azt intézték annak teljesítésére nem rendelkezik hatáskörrel, hivatalból megküldi azt az illetékes nemzeti hatósághoz és a megkereső Felet erről közvetlenül tájékoztatja.

d) A jelen bekezdés alapján előterjesztett és kényszerintézkedés megtételét nem igénylő kérelmeket és tájékoztatásokat a megkereső Fél hatáskörrel rendelkező

hatóságai közvetlenül küldhetik meg a megkeresett Fél hatáskörrel rendelkező hatóságainak.

e) A jelen Egyezmény aláírása vagy a megerősítő, elfogadó, jóváhagyó vagy csatlakozási okmányok letétbe helyezése alkalmával mindegyik Szerződő Fél tájékoztathatja az Európa Tanács Főtitkárát, hogy célszerűségi okokból a jelen bekezdés alapján előterjesztett kérelmeket központi hatóságához kell intézni.

*28. Cikk*
*Titkosság és a felhasználás korlátozása*

1. A jelen Cikkben foglalt rendelkezéseket kell alkalmazni jogsegélyszerződés vagy a megkereső Fél és a megkeresett Fél között hatályban lévő egységes vagy kölcsönös jogi szabályozáson alapuló megállapodás hiányában. Jelen Cikk rendelkezéseit nem kell alkalmazni, amennyiben létezik hasonló jellegű szerződés, megállapodás vagy jogi szabályozás, kivéve ha az érintett Felek azok helyett a jelen Cikkben foglalt rendelkezések részleges vagy teljes alkalmazása mellett döntenek.

2. A megkeresett Fél a megkeresésre válaszul az információk megküldését, illetőleg az anyagok átadását ahhoz a feltételhez kötheti, hogy

a) az információkat tartsák titokban, ha a jogsegélykérelmet ezen feltétel hiányában nem lehetne teljesíteni; vagy

b) azokat nem használhatják fel olyan nyomozásban vagy eljárásban, amely a jogsegélykérelemben meghatározottól eltér.

3. Ha a megkereső Fél nem tudja teljesíteni a 2. bekezdésben meghatározott feltételt, haladéktalanul tájékoztatnia kell erről a megkeresett Felet, aki dönt arról, hogy ennek ellenére átadja-e az információt vagy sem. Ha a megkereső Fél elfogadja a feltételt, akkor ezt követően a feltétel szerint köteles eljárni.

4. A Szerződő Fél, aki a 2. bekezdésben meghatározott feltétel szerint ad át információt vagy dolgot, kérheti, hogy a másik Fél a feltétellel kapcsolatban pontosan közölje, hogy az információt vagy a dolgot mire kívánja felhasználni.

## IV. FEJEZET
## KÜLÖNÖS RENDELKEZÉSEK

### *I. Cím*
### *Ideiglenes intézkedésekkel kapcsolatos jogsegély*

*29. Cikk*
*Tárolt számítástechnikai adat gyors megőrzése*

1. A Fél megkeresheti a másik Felet, hogy rendelje el vagy más módon kényszerítse ki a területén található számítástechnikai rendszer útján tárolt adatok gyors megőrzését, melyekkel kapcsolatban az átvizsgálásra vagy más hasonló hozzáférésre, lefoglalásra vagy más hasonló megszerzésre, illetőleg átadásra a megkereső Fél jogsegélykérelmet kíván előterjeszteni.

2. Az 1. bekezdés alapján előterjesztett megőrzés iránti kérelemnek a következő adatokat kell tartalmaznia:

a) a megőrzést kérő hatóságot;

b) a nyomozás vagy a büntetőeljárás tárgyául szolgáló bűncselekményt és a vonatkozó tények rövid ismertetését;

c) a megőrizni kért tárolt adatokat és azok bűncselekménnyel való kapcsolatát;

d) a számítástechnikai adatok birtokosát vagy a számítástechnikai rendszer helyét azonosító valamennyi hozzáférhető információt;

e) a megőrzés szükségességét; és

f) a tényt, hogy a Fél jogsegélykérelmet kíván előterjeszteni a tárolt számítástechnikai adatok átvizsgálása vagy más hasonló hozzáférés, azok lefoglalása vagy más hasonló módon történő biztosítása, illetve átadása érdekében.

3. A megkeresett Fél, a másik Fél által előterjesztett kérelem megérkezését követően, megteszi azon intézkedéseket, melyek belső jogával összhangban a meghatározott adatok megőrzésére vonatkozó eljárás haladéktalan lefolytatásához szükségesek. A kérelemre történő válaszadás körében a megőrzésnek nem előzetes feltétele a cselekmény mindkét Fél részéről fennálló büntethetősége.

4. A Szerződő Fél, aki a tárolt adatok átvizsgálására vagy más hasonló hozzáférésre, lefoglalásra vagy más hasonló megszerzésre, illetőleg az átadásra vonatkozó megkeresésre történő válaszadás feltételeként megköveteli a mindkét Fél részéről fennálló büntethetőséget, a jelen Egyezmény 2-11. Cikkeiben nem szereplő bűncselekmények vonatkozásában fenntarthatja azt a jogot, hogy elutasítja a jelen Cikken alapuló megőrzésre vonatkozó kérelmet abban az esetben, ha alappal feltételezheti, hogy az adatok átadásakor nem teljesül majd a mindkét Fél részéről fennálló büntethetőségi feltétel.

5. A megőrzési kérelem teljesítése továbbá kizárólag abban az esetben tagadható meg:

a) ha a kérelem olyan bűncselekményre vonatkozik, amelyet a megkeresett Fél politikai bűncselekménynek, vagy politikai bűncselekménnyel összefüggő bűncselekménynek tekint;

b) ha a megkeresett Fél úgy ítéli meg, hogy a kérelem teljesítése sértheti országa szuverenitását, biztonságát, közrendjét vagy más lényeges érdekeit.

6. Ha a megkeresett Fél úgy ítéli meg, hogy a megőrzés nem biztosítja megfelelően az adatok későbbi hozzáférhetőségét, vagy veszélyezteti a megkereső Fél nyomozásának titkosságát, illetőleg más módon hátrányosan befolyásolja azt,

ebben az esetben haladéktalanul értesíti a megkereső Felet, aki dönt arról, hogy kéri-e mindezek ellenére a kérelem teljesítését.

7. Az 1. bekezdés szerinti kérelem alapján végrehajtott megőrzés legfeljebb 60 napig tart annak érdekében, hogy lehetővé tegye a megkereső Fél részére, hogy az adatok átvizsgálására vagy más hasonló hozzáférésére, lefoglalására vagy más hasonló megszerzésére, illetőleg átadására irányuló megkeresést terjeszthessen elő. A kérelem megérkezését követően az adatokat meg kell őrizni annak elbírálásáig.

*30. Cikk*
*Megőrzött forgalmi adat gyors átadása*

1. Meghatározott kommunikációhoz kapcsolódó, forgalmi adat megőrzésére irányuló, a 29. Cikken alapuló megkeresés teljesítése esetén, ha a megkeresett Fél megállapítja, hogy egy másik Államban található szolgáltató is részt vett a kommunikáció továbbításában, a megkeresett Fél megfelelő mennyiségű forgalmi adatot haladéktalanul átad a megkereső Félnek a kommunikáció továbbítására igénybe vett útvonal és a szolgáltató azonosítása érdekében.

2. Az 1. bekezdés alkalmazásával a forgalmi adat átadására irányuló megkeresés teljesítése kizárólag abban az esetben tagadható meg, ha:

a) a megkeresés olyan bűncselekményre vonatkozik, amelyet a megkeresett Fél politikai bűncselekménynek, vagy politikai bűncselekménnyel összefüggő bűncselekménynek tekint;

b) a megkeresett Fél úgy ítéli meg, hogy a megkeresés teljesítése sértheti országa szuverenitását, biztonságát, közrendjét vagy más lényeges érdekeit.

## *II. Cím*
## *Nyomozati jogkörökkel kapcsolatos jogsegély*

*31. Cikk*
*Tárolt számítástechnikai adathoz való hozzáférésre vonatkozó jogsegély*

1. A Szerződő Fél megkeresheti a másik Felet, hogy a területén található számítástechnikai rendszer útján tárolt adatokat átvizsgálja vagy azokhoz más hasonló módon férjen hozzá, foglalja le vagy más hasonló módon szerezze meg, illetőleg adja át, ideértve a 29. Cikk alapján megőrzött adatokat is.

2. A megkeresett Fél a 23. Cikkben hivatkozott nemzetközi okmányokban, megállapodásokban, és a nemzeti jogokban foglaltakat alkalmazva, a jelen részben meghatározott rendelkezésekkel összhangban teljesíti a megkeresést.

3. A megkeresést a lehető legrövidebb időn belül kell teljesíteni:

a) ha alappal feltételezhető, hogy az érintett adatokat módosulás vagy megsemmisülés veszélyezteti, vagy

b) a 2. bekezdésben hivatkozott jogi eszközök, megállapodások és jogi szabályozás, gyors együttműködést írnak elő.

*32. Cikk*
*Tárolt számítástechnikai adathoz való hozzáférés határokra tekintet nélkül, hozzájárulás vagy nyilvános elérhetőség esetén*

A Szerződő Fél a másik Szerződő Fél engedélye nélkül:

a) a nyilvánosság számára elérhető módon (nyílt forrású) tárolt számítástechnikai adathoz hozzáférhet, függetlenül az adat földrajzi elhelyezkedésétől; vagy

b) a másik Szerződő Fél területén tárolt számítástechnikai adathoz hozzáférhet vagy a területén levő számítástechnikai rendszer útján azt megszerezheti, amennyiben a Fél beszerzi az adat számítástechnikai rendszer útján történő átadására jogszabályban feljogosított személy önkéntes és jogszerű hozzájárulását.

*33. Cikk*
*Forgalmi adat valós idejű összegyűjtésével kapcsolatos jogsegély*

1. A Szerződő Felek kölcsönösen jogsegélyt nyújtanak egymásnak a területükhöz kötődő, számítástechnikai rendszer útján továbbított meghatározott kommunikációval összefüggő forgalmi adat valós idejű összegyűjtésében. A jogsegély a 2. bekezdésben meghatározott követelmények alapján, a belső jog feltételei és eljárásai szerint történik.

2. Minden Szerződő Fél segítséget nyújt legalább azon bűncselekményekkel kapcsolatban, melyekhez a belső jogban szabályozott hasonló bűncselekmény esetén a forgalmi adatokat valós időben össze lehet gyűjteni.

*34. Cikk*
*Tartalomra vonatkozó adat kifürkészésére vonatkozó jogsegély*

A Szerződő Felek vonatkozó megállapodásaik és belső jogi szabályozásuk által lehetővé tett mértékben, kölcsönösen jogsegélyt nyújtanak egymásnak a számítástechnikai rendszerben továbbított, meghatározott kommunikációk tartalmára vonatkozó adatok valós idejű összegyűjtésében és rögzítésében.

## *III. Cím*
## *A 24/7 hálózat*

*35. Cikk*
*A 24/7 hálózat*

1. Minden Szerződő Fél kijelöl egy éjjel-nappal, a hét minden napján elérhető kapcsolattartási pontot, annak érdekében, hogy lehetővé tegye a számítástechnikai adatokkal és rendszerrel összefüggő bűncselekményekre vonatkozó nyomozásokkal, vagy a bűncselekményekre vonatkozó elektronikus bizonyítékok összegyűjtésével

kapcsolatos azonnali segítségnyújtást. Ez a segítségnyújtás felöleli a következő intézkedések megkönnyítését, vagy, ha azt a belső jog és a gyakorlat lehetővé teszi, közvetlen foganatosítását:

a) technikai tanácsok átadása;

b) adatok megőrzése a 29. és 30. Cikk szerint;

c) bizonyítékok összegyűjtése, jogi információk átadása és a gyanúsítottak tartózkodási helyének meghatározása.

2. a) A Fél kapcsolattartási pontja számára biztosítani kell azokat az eszközöket, hogy késedelem nélkül tarthassa a kapcsolatot a másik Fél kapcsolattartási pontjával.

b) Ha a Fél által kijelölt kapcsolattartási pont független a Fél nemzetközi jogsegélyért vagy kiadatásért felelős hatósága(i)tól, a kapcsolattartási pontnak alkalmasnak kell lennie ezen hatóság(ok)kal történő késedelem nélküli együttműködésre.

3. A hálózat működtetésének megkönnyítése érdekében minden Szerződő Fél biztosítja a képzett és megfelelően felszerelt személyzetet.

## NEGYEDIK RÉSZ
## ZÁRÓ RENDELKEZÉSEK

### *36. Cikk*
### *Aláírás és hatályba lépés*

1. Jelen Egyezmény az Európa Tanács tagállamai valamint az Egyezmény kidolgozásában részt vett nem tagállamok részére áll nyitva aláírásra.

2. A jelen Egyezményt megerősíteni, elfogadni vagy jóváhagyni lehet. A megerősítő, elfogadási vagy jóváhagyási okmányokat az Európa Tanács Főtitkáránál kell letétbe helyezni.

3. Jelen Egyezmény hatályba lépésének napja az azon időpontot követő három hónap utáni naptári hónap első napja, amikor öt Állam, közülük legalább három az Európa Tanács tagja, egyetértését fejezte ki azzal, hogy az Egyezmény az 1. és 2. bekezdésekben foglalt rendelkezéseknek megfelelően kötelező legyen számára.

4. Mindazon aláíró Államok vonatkozásában, akik egyetértésükkel ezt követően ismerik el kötelezőnek azt, az Egyezmény az 1. és 2. bekezdésében foglaltak szerinti, kötelező erővel való egyetértés kinyilvánításától számított három hónapot követő naptári hónap első napján lép hatályba.

### *37. Cikk*
### *Csatlakozás az Egyezményhez*

1. Jelen Egyezmény hatályba lépését követően az Európa Tanács Miniszteri Bizottsága, az Egyezmény Szerződő Államaival folytatott konzultáció és a Szerződő Államok képviselői egyhangú határozata alapján csatlakozásra kérhet fel minden olyan Államot, mely nem tagja az Európa Tanácsnak és nem vett részt az Egyezmény kidolgozásában. A döntést az Európa Tanács Alapszabályának 20. d) Cikke szerinti többséggel, valamint a Miniszteri Bizottságban képviseletre jogosult Szerződő Államok képviselőinek egyhangú határozatával kell meghozni.

2. Az 1. bekezdés alapján csatlakozó Államok vonatkozásában az Egyezmény a csatlakozási okmánynak az Európa Tanács Főtitkáránál történt letétbe helyezés időpontjától számított három hónapot követő naptári hónap első napján lép hatályba.

*38. Cikk*
*Területi alkalmazás*

1. Az Egyezmény aláírása vagy a megerősítő, elfogadó, jóváhagyó vagy csatlakozási okmányok letétbe helyezése alkalmával minden Állam megnevezheti azt a területet vagy területeket, ahol a jelen Egyezményt alkalmazni fogják.

2. Minden Állam kiterjesztheti a jelen Egyezmény alkalmazását egy későbbi időpontban az Európa Tanács Főtitkárához intézett nyilatkozatában az abban meghatározott más területre. Az ilyen terület vonatkozásában az Egyezmény a nyilatkozat Főtitkár általi kézhezvételét követő három hónapot követő naptári hónap első napján lép hatályba.

3. Az 1. és 2. bekezdés alapján tett, meghatározott területre vonatkozó bármely nyilatkozatot a Főtitkárhoz címzett értesítéssel vissza lehet vonni. A visszavonás a Főtitkárhoz eljuttatott értesítés kézhezvételét követő három hónapot követő naptári hónap első napján lép hatályba.

*39. Cikk*
*Az Egyezmény hatása*

1. Jelen Egyezmény célja, hogy kiegészítse a Szerződő Felek között fennálló két- vagy többoldalú szerződéseket, illetve megállapodásokat, ideértve a következő egyezményeket is:

- a Strasbourgban, 1957. december 13-án kelt, Európai kiadatási egyezményt [ESZS N 24]

- a Strasbourgban, 1959. április 20-án kelt, a Kölcsönös Bűnügyi Jogsegélyről szóló európai egyezményt [ESZS N 30]

- a Strasbourgban, 1978. március 17-én kelt, a Kölcsönös Bűnügyi Jogsegélyről szóló európai egyezmény Kiegészítő jegyzőkönyvét [ESZS N 99]

2. Ha két vagy több Szerződő Fél a jelen Egyezmény által szabályozott kérdésekre vonatkozóan korábban már kötött egymással szerződést vagy megállapodást, illetve ezen tárgykör vonatkozásában más módon rendezték

kapcsolataikat, vagy a jövőben kell ezt megtenniük, akkor lehetőségük van arra is, hogy az említett szerződést vagy megállapodást alkalmazzák, illetőleg a kapcsolatuk szabályai szerint járjanak el. Ha a Szerződő Felek az Egyezmény rendelkezéseitől eltérően alakították ki a jelen Egyezmény által szabályozott kérdéseket érintő kapcsolataikat, akkor biztosítaniuk kell, hogy ezek összeegyeztethetőek legyenek az Egyezmény alapelveivel és céljaival.

3. A jelen Egyezmény egyetlen rendelkezése sem érinti a Szerződő Fél egyéb jogait, korlátozásait, kötelezettségeit, illetve felelősségét.

*40. Cikk*
*Nyilatkozatok*

Az Egyezmény aláírása vagy a megerősítő, elfogadó, jóváhagyó vagy csatlakozási okmányok letétbe helyezése alkalmával mindegyik Állam az Európa Tanács Főtitkárához intézett írásbeli nyilatkozatában biztosíthatja magának azt a lehetőséget, hogy a 2. és 3. Cikkben, a 6. Cikk 1. bekezdésének b) pontjában, a 7. Cikkben, a 9. Cikk 3. bekezdésében, valamint a 27. Cikk 9. bekezdésének e) pontjában meghatározott feltételeken túl egy vagy több további feltételt követeljen meg.

*41. Cikk*
*Szövetségi záradék*

1. A Szövetségi Állam fenntarthatja magának azt a jogot, hogy a jelen Egyezmény II. Részében meghatározott kötelezettségeket annyiban vállalja, amennyiben azok összeegyeztethetők a központi kormányzat és a tagállamok, vagy más hasonló területi egységek viszonyát meghatározó alapvető elvekkel, feltéve, hogy biztosított a Szövetségi Állam együttműködése a III. Részben meghatározottak szerint.

2. Ha a Szövetségi Állam az 1. bekezdés alapján fenntartást tesz, a fenntartás rendelkezéseit nem fogalmazhatja meg akként, hogy azzal kizárja vagy jelentősen korlátozza a II. Részben meghatározott intézkedésekre vonatkozó kötelezettségeit. A Szövetségi Államnak széleskörű és hatékony eszközöket kell biztosítania annak érdekében, hogy lehetővé tegye a II. Részben meghatározott intézkedések megtételét.

3. Ha az Egyezmény rendelkezéseinek alkalmazása az egyes tagállamok vagy más hasonló területi egységek jogalkotási jogkörébe tartozik, amelyek ugyanakkor a szövetségi alkotmányos rendszer alapján nem kötelesek jogalkotási intézkedéseket hozni, a szövetségi kormányzat tájékoztatja a tagállamok illetékes hatóságait az említett rendelkezésekről, közli támogató véleményét és ösztönzi őket azok alkalmazását lehetővé tevő intézkedések elfogadására.

*42. Cikk*
*Fenntartások*

Az Egyezmény aláírása vagy a megerősítő, elfogadó, jóváhagyó vagy csatlakozási okmányok letétbe helyezése alkalmával mindegyik Állam az Európa

Tanács Főtitkárához intézett írásbeli nyilatkozatában a 4. Cikk 2. bekezdésében, a 6. Cikk 3. bekezdésében, a 9. Cikk 4. bekezdésében, a 10. Cikk 3. bekezdésében, a 11. Cikk 3. bekezdésében, a 14. Cikk 3. bekezdésében, a 22. Cikk 2. bekezdésében, a 29. Cikk 4. bekezdésében, valamint a 41. Cikk 1. bekezdésében meghatározott fenntartásokat teheti. Más fenntartást nem lehet tenni.

*43. Cikk*
*Fenntartások hatálya és visszavonása*

1. A Szerződő Fél jogosult a 42. Cikkben foglaltakkal összhangban tett fenntartás részleges vagy teljes visszavonására az Európa Tanács Főtitkárához intézett nyilatkozat útján. A visszavonás a Főtitkárhoz eljuttatott nyilatkozat kézhezvétele időpontjában lép hatályba. Ha a nyilatkozat a fenntartás visszavonásának hatályba lépését a Főtitkár általi kézhezvételt követő időponthoz köti, a visszavonás a meghatározott későbbi időpontban lép hatályba.

2. A Fél a 42. Cikkben foglaltakkal összhangban tett fenntartását, amint a körülmények lehetővé teszik, részben vagy egészben visszavonja.

3. Az Európa Tanács Főtitkára rendszeresen tájékoztatást kérhet a 42. Cikk szerinti fenntartás(oka)t tett Féltől a fenntartás(ok) visszavonásának lehetséges esélyeiről.

*44. Cikk*
*Módosítások*

1. Mindegyik Szerződő Fél indítványozhatja a jelen Egyezmény módosítását; az Európa Tanács Főtitkára valamennyi módosító indítványról értesíti az Európa Tanács tagállamait, az Egyezmény kidolgozásában részt vett nem tagállamokat, valamint valamennyi, az Egyezményhez csatlakozott, vagy a 37. Cikkben foglalt rendelkezéseknek megfelelően a csatlakozásra meghívott Államot.

2. Minden módosítási indítványt közölni kell a Büntetőjogi Kérdésekkel Foglalkozó Európai Bizottsággal (CDPC) is, mely az indítványozott módosítással kapcsolatos véleményét közli a Miniszteri Bizottsággal.

3. A Miniszteri Bizottság megvizsgálja a módosító indítványt és a CDPC által előterjesztett véleményt, majd a nem tagállam Szerződő Felekkel folytatott konzultációt követően elfogadhatja a módosítást.

4. A Miniszteri Bizottság által a jelen Cikk 3. bekezdése szerint elfogadott valamennyi módosítás szövegét az elfogadás érdekében meg kell küldeni a Szerződő Feleknek.

5. A jelen Cikk 3. bekezdése szerint elfogadott valamennyi módosítás az azt követő harmincadik napon lép hatályba, hogy mindegyik Szerződő Fél értesítette a Főtitkárt a módosítás elfogadásáról.

*45. Cikk*
*A viták rendezése*

1. A Büntetőjogi Kérdésekkel Foglalkozó Európai Bizottságot (CDPC) tájékoztatni kell a jelen Egyezmény értelmezéséről és alkalmazásáról.

2. A Szerződő Felek között a jelen Egyezmény értelmezése és alkalmazása tekintetében felmerülő bármely vita esetében a Felek a vitás kérdéseket tárgyalás vagy a választásuk szerinti bármely más békés eszköz útján törekednek rendezni, ideértve az érintett Felek közötti megállapodás értelmében a vitának a Büntetőjogi Kérdésekkel Foglalkozó Európai Bizottság elé, a Szerződő Felekre kötelező döntést hozó választott bíróság elé, illetőleg a Nemzetközi Bíróság elé terjesztését is.

*46. Cikk*
*Egyeztetés a Felek között*

1. A Szerződő Felek szükség szerint rendszeresen egyeztetnek annak érdekében, hogy megkönnyítsék:

a) a jelen Egyezmény tényleges alkalmazását és megvalósítását, ide értve a tárgykörrel kapcsolatban felmerült problémák azonosítását, valamint az Egyezményhez fűzött fenntartások és nyilatkozatok hatásának vizsgálatát;

b) a számítástechnikai bűnözés területén felmerült, jelentős jogi, politikai és technikai fejlődésre vonatkozó információk cseréjét és az elektronikus formában megjelenő bizonyítékok összegyűjtését;

c) az Egyezmény kiegészítése vagy módosítása lehetőségének megfontolását.

2. A Büntetőjogi Kérdésekkel Foglalkozó Európai Bizottságot (CDPC) rendszeresen tájékoztatni kell az 1. bekezdésben meghatározott egyeztetések eredményéről.

3. A CDPC szükség szerint elősegíti az 1. bekezdésben meghatározott egyeztetést, és a szükséges intézkedések meghozatalával segítséget nyújt az Egyezményt módosítani vagy kiegészíteni kívánó Feleknek. Legkésőbb a jelen Egyezmény hatálybelépését követő három év elteltével a CDPC a Szerződő Felekkel együttműködve az Egyezmény rendelkezéseit felülvizsgálja és ha szükséges, megfelelő módosításokat ajánl.

4. Az 1. bekezdés rendelkezéseinek alkalmazása során felmerült költségeket közösen meghatározott módon a Szerződő Felek viselik, kivéve, ha azokat az Európa Tanács átvállalja.

5. Az Európa Tanács Titkársága segítséget nyújt a Feleknek a jelen Cikkből származó jogkörök gyakorlásában.

*47. Cikk*
*Felmondás*

1. Minden Szerződő Fél az Európa Tanács Főtitkárához intézett értesítéssel felmondhatja a jelen Egyezményt.

2. A felmondás a Főtitkárhoz eljuttatott értesítés kézhezvételét követő három hónapot követő naptári hónap első napján lép hatályba.

*48. Cikk*
*Értesítések*

Az Európa Tanács Főtitkára értesíti az Európa Tanács tagállamait, a jelen Egyezmény kidolgozásában részt vett nem tagállamokat, valamint valamennyi, az Egyezményhez csatlakozott vagy a csatlakozásra meghívott Államot:

a) az Egyezmény minden egyes aláírásáról;

b) minden egyes megerősítési, elfogadási, jóváhagyási vagy csatlakozási okirat letétbe helyezéséről;

c) a jelen Egyezmény 36. és 37. Cikkeivel összhangban történt minden hatálybalépésről;

d) a 40. Cikk alapján tett minden egyes nyilatkozatról vagy a 42. Cikk alapján tett minden egyes fenntartásról;

e) a jelen Egyezménnyel kapcsolatos minden értesítésről, nyilatkozatról vagy más okmányról.

Fentiek hiteléül az erre kellőképpen felhatalmazott alulírottak a jelen Egyezményt aláírták.

Kelt Budapesten, 2001. november 23-án, angol és francia nyelven, mindkét szöveg egyaránt hiteles, egyetlen példányban, amely az Európa Tanács levéltárában marad letétbe helyezve. Az Európa Tanács Főtitkára hiteles másolatot küld az Európa Tanács valamennyi tagállamának, jelen Egyezmény kidolgozásában részt vett nem tagállamoknak, valamint valamennyi, az Egyezményhez csatlakozásra meghívott Államnak.”

**3. §**

(1) A Magyar Köztársaság Kormánya az Országgyűlés felhatalmazása alapján az Egyezmény megerősítéséről szóló okirat letétbe helyezésekor az Egyezmény 9. Cikkéhez a következő fenntartást tette:

„A 9. Cikk 4. bekezdésében foglaltak alapján Magyarország fenntartja a jogot arra, hogy nem alkalmazza a 9. Cikk 2. bekezdésének b) pontját.”

(2) A Magyar Köztársaság Kormánya az Országgyűlés felhatalmazása alapján az Egyezmény megerősítéséről szóló okirat letétbe helyezésekor a következő nyilatkozatokat tette:

Az Egyezmény 24. Cikkéhez:

„A 24. Cikk 7. bekezdésének a) pontja értelmében Magyarország tájékoztatja az Európa Tanács Főtitkárát, hogy kiadatási szerződés hiányában a kiadatási kérelem, illetőleg az ideiglenes kiadatási letartóztatásra irányuló kérelem előterjesztésére vagy elfogadására az Igazságügyi Minisztérium jogosult. Az Interpol Magyar Nemzeti Iroda kizárólag az ideiglenes kiadatási letartóztatásra vonatkozó kérelmek előterjesztésére és fogadására jogosult.”

Az Egyezmény 27. Cikkéhez:

„A 27. Cikk 2. bekezdésének a) és c) pontja alapján Magyarország tájékoztatja az Európa Tanács Főtitkárát, hogy központi hatóságként a büntetőeljárás megindítását megelőzően érkezett megkeresések tekintetében az Országos Rendőr-főkapitányságon működő Nemzetközi Bűnügyi Együttműködési Központot (NEBEK), míg a büntetőeljárás megindítását követően foganatosított megkeresések tekintetében a Magyar Köztársaság Legfőbb Ügyészségét jelöli ki.”

„A 27. Cikk 9. bekezdésének e) pontja értelmében Magyarország tájékoztatja az Európa Tanács Főtitkárát, hogy célszerűségi okokból a 27. Cikk 9. bekezdése alapján előterjesztett kérelmeket a központi hatósághoz kell intézni.”

Az Egyezmény 35. Cikkéhez:

„A 35. Cikk alapján Magyarország tájékoztatja az Európa Tanács Főtitkárát, hogy a hét minden napján, éjjel-nappal elérhető kapcsolattartási pontként az Országos Rendőr-főkapitányságon működő Nemzetközi Bűnügyi Együttműködési Központot (NEBEK) jelöli ki.”

**4. §**

E törvény a kihirdetése napján lép hatályba, azonban az Egyezmény rendelkezéseit 2004. július 1-jétől kell alkalmazni.

# INDOKOLÁS

## az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai bűnözésről szóló Egyezményének kihirdetéséről szóló törvényjavaslathoz

### Általános Indokolás

1. A számítástechnika felhasználási lehetőségeinek széles körű, a mindennapi élet mind több tevékenységi szintjét átfogó elterjedésével, a számítástechnikai rendszerek közvetlen, határokon átívelő kapcsolatát biztosító világháló kialakulásával és fejlődésével egyidejűleg - sajnálatosan - nemzetközi szinten és hazánkban is egyre nagyobb teret nyer a számítástechnikai bűnözés. A szervezett bűnözés is azonnal felismerte a számítástechnika jelentőségét, így a határon átnyúló bűnelkövetések egyik legfontosabb eszközévé a számítógép és a világháló vált. A mindeddig nem tapasztalt nagyságú és sebességű adatáramlást, valamint kommunikációt lehetővé tevő Internet napjainkra az ellenőrizhetetlen pénzmozgások egyik fő színtere lett. A világhálón lebonyolított pénzmosás mellett a közintézmények és magánszemélyek elleni számítógépes támadások is a nemzetközi bűnözés egyik új és rohamosan fejlődő területét jelentik.

Az Európa Tanács, felismerve a számítástechnikai rendszereken és a világhálón megvalósuló bűnözés elleni összehangolt nemzetközi fellépés fontosságát, alkotta meg a Számítástechnikai bűnözésről szóló Egyezményt (a továbbiakban: Egyezmény).

2. Az Egyezmény előkészítésével párhuzamosan Magyarországon is megkezdődött a büntető anyagi és eljárásjogi normák területén szükséges módosítások kidolgozása, annak érdekében, hogy az Egyezmény aláírását követő legrövidebb időn belül hazánk büntetőjogi rendszere teljes összhangban legyen az Egyezmény rendelkezéseivel.

A büntető anyagi jog területén a Büntető Törvénykönyvről szóló 1978. évi IV. törvényt (a továbbiakban: Btk.) módosító 2001. évi CXXI. törvény iktatta be a Btk.-ba az Egyezmény rendelkezéseivel összhangban álló új szabályokat, tényállásokat. A módosított, illetőleg új rendelkezések 2002. április 1-jén léptek hatályba.

A büntetőeljárási jog területén a büntetőeljárásról szóló 1998. évi XIX. törvényt (a továbbiakban: Be.) átfogóan módosító 2002. évi I. törvény vezetett be az Egyezmény rendelkezéseinek megfelelő szabályokat, illetőleg teremtette meg egy új kényszerintézkedés eljárásjogi alapjait. A módosított, illetve új rendelkezések 2003. július 1-jén léptek hatályba.

3. Az Egyezmény az 1. Cikkben meghatározza az egyes anyagi jogi tényállásokban, illetőleg az eljárásjogi rendelkezések esetében használt kifejezések pontos tartalmát, többek között az „informatikai rendszer” fogalmát is. Az informatikai bűncselekményeket pönalizáló új büntetőjogi tényállások vonatkozásában a Btk. 300/F. §-a határozza meg - az Egyezmény rendelkezéseivel összhangban - a számítástechnikai rendszer fogalmát.

Az Egyezmény az értelmező rendelkezések alkotta első rész mellett a második részben határozza meg a nemzeti szinten meghozandó jogalkotási intézkedéseket.

Az első fejezetben azokat a cselekményeket határozza meg, amelyeket a szerződő államoknak bűncselekménnyé kell nyilvánítani.

Az Egyezmény 2. Cikke büntetőjogi szankció alkalmazását követeli meg a számítástechnikai rendszerbe történő jogosulatlan és szándékos belépéssel szemben. Az Egyezménnyel összhangban a Btk. 300/C. §-ában meghatározott számítástechnikai rendszer és adatok elleni bűncselekmény (1) bekezdése büntetendő cselekménnyé nyilvánítja a számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedések megsértésével vagy kijátszásával történő jogosulatlan belépést, valamint az engedélyezett belépést követően a jogosultság kereteit túllépő, illetőleg azt más módon megsértő bennmaradást is.

Az Egyezmény 3. Cikke büntetni rendeli a számítástechnikai rendszerben tárolt vagy annak útján továbbított számítástechnikai adatok jogosulatlan kifürkészését. A Btk. 178/A. §-ában meghatározott magántitok jogosulatlan megismerése bűncselekményi tényállása a módosítás után lehetővé teszi a számítástechnikai úton továbbított adatok, közlemények jogosulatlan kifürkészőinek büntetőjogi felelősségre vonását.

Az Egyezmény 4. Cikkével – amely az adatok jogosulatlan törlését, megváltoztatását szankcionálja – és 5. Cikkével – amely a számítástechnikai rendszer működésének jogosulatlan akadályozását nyilvánítja bűncselekménnyé – összhangban a Btk. 300/C. §-ában meghatározott számítástechnikai rendszer és adatok elleni bűncselekmény (2) bekezdésének a) és b) pontja rendeli büntetni az Egyezményben meghatározott cselekményeket.

Az Egyezmény 6. Cikke önálló, sui generis bűncselekményként rendeli büntetni a nemzeti jogokban a számítástechnikai eszközökkel történő visszaélést, azaz a számítástechnikai program, jelszó, belépési kód, vagy a számítástechnikai rendszerbe való belépést lehetővé tevő adatnak, berendezésnek számítástechnikai bűncselekmények elkövetése érdekében történő készítését, megszerzését, forgalomba hozatalát, az azzal való kereskedést, vagy más módon történő hozzáférhetővé tételét. Az egyezményi szabályokkal teljes mértékben összhangban áll a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása elnevezésű, a Btk. 300/E. §-ában meghatározott önálló bűncselekményi tényállás.

A 7. Cikkben meghatározott számítástechnikai hamisítás bűncselekménye a magyar jogrendszerben az elektronikus aláírásról szóló 2001. évi XXXV. törvény hatálybalépésével vált büntetendő cselekménnyé. A hivatkozott törvény a Polgári perrendtartásról szóló 1952. évi III. törvény 196. §-ának (1) bekezdése e) és f) pontjába, a magánokiratok körébe beiktatta az elektronikus okiratot. Az elektronikus okirat Egyezmény szerinti meghamisítása így a Btk. 276. §-ába ütköző magánokirat-hamisítás bűncselekményét valósítja meg.

Az Egyezmény 8. Cikkében meghatározott számítástechnikai csalás bűncselekményének megfelelően módosult rendelkezésekkel került

újraszabályozásra a Btk. 300/C. §-ának (3) és (4) bekezdésében a számítástechnikai rendszer útján elkövetett csalás.

Az Egyezmény 9. Cikkében – a teljes körű és általános tilalom elvéből kiindulva – önálló tényállásként szabályozza a gyermek-pornográfiával kapcsolatos, számítástechnikai rendszer útján megvalósuló cselekményeket, többek között megkövetelve a gyermek-pornográfia készítése mellett a számítástechnikai rendszer útján történő felajánlásnak, hozzáférhetővé tételnek és az ilyen termékek birtoklásának büntetendővé nyilvánítását is.

A Btk. 195/A. §-a az Egyezmény 9. Cikkében foglaltaknak megfelelően a tiltott pornográf felvétel vagy felvételek vonatkozásában az Egyezményben meghatározott valamennyi elkövetési magatartást bűncselekménnyé nyilvánítja.

Az Egyezmény 9. Cikke 2. bekezdésének b) pontjában gyermek-pornográfiaként határozza meg az olyan pornográf terméket is, amely vizuális úton ábrázol kifejezetten szexuális magatartást tanúsító kiskorúnak tűnő személyt.

A magyar büntetőjogi szabályozás az Egyezmény általános és teljes körű tilalmától eltérően kifejezetten csak a kiskorú személyeket védi a fényképek, digitális képek készítésében megjelenő szexuális kizsákmányolással szemben. A magyar büntetőjog a felnőttkorúakról készített pornográf ábrázolásokat akkor sem tekinti bűncselekménynek, ha a felnőttkorú személy kiskorúnak tűnik a felvételen. A magyar büntetőjogi szabályozásnak a hivatkozott bűncselekményi tényálláshoz kötődő alapelveire és az említett törvényi tényállás által védett jogtárgy természetére tekintettel az Egyezmény 9. Cikke 4. bekezdésében foglaltak alapján a megerősítő okmány letétbe helyezésekor Magyarország fentartással zárta ki a 9. Cikk 2. bekezdése b) pontjának hazai alkalmazását.

Az Egyezmény 10. Cikkében rendelkezéseket tartalmaz a szerzői és szomszédos jogok megsértésével kapcsolatos, számítástechnikai rendszer útján elkövetett bűncselekményekre vonatkozóan. A Btk. 329/A. §-ában meghatározott „Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése” tényállása teljes mértékben megfelel az Egyezmény hivatkozott cikkében foglalt követelményeknek.

Az Egyezmény 11. Cikke szerint a felsorolt cselekmények kísérletét, valamint a bűncselekmények elkövetéséhez kapcsolódó bűnrészességet is büntetendővé kell nyilvánítani, mely követelménynek a Btk. szabályozása maradéktalanul megfelel.

Az Egyezmény 12. Cikke szerint mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, amelyek ahhoz szükségesek, hogy az Egyezményben foglalt bűncselekményekkel kapcsolatban a jogi személyek felelősségre vonhatók legyenek, ha a jogi személy képviseletét, igazgatását vagy ellenőrzését ellátó személy e minőségében követte el a felsorolt bűncselekményeket. A jogi személy felelőssége büntetőjogi, polgári jogi vagy közigazgatási jogi lehet.

A jogi személyekkel szemben alkalmazható büntetőjogi intézkedésekről szóló 2001. évi CIV. törvény megteremti annak lehetőségét, hogy a jogi személyekkel szemben – a törvényben meghatározott feltételek fennállása esetén – büntetőjogi intézkedésként a jogi személy megszüntetését, tevékenységének korlátozását

rendeljék el, vagy pénzbírságot szabjanak ki vele szemben. A törvény rendelkezései megfelelnek az Egyezmény előírásainak és az Európai Unióhoz történő csatlakozásunkról szóló nemzetközi szerződést kihirdető törvény hatályba lépésével egyidejűleg hatályba is lépett.

Az Egyezmény második fejezete a számítástechnikai bűncselekmények alapján indult nyomozás és büntetőeljárás eredményességének elősegítése, illetőleg az elektronikus formában megjelenő bizonyítékok hatékonyabb felderítése, összegyűjtése érdekében új eljárásjogi intézmények bevezetését, illetőleg a már szabályozott nyomozati és eljárási cselekmények rendelkezéseinek módosítását, kiegészítését írja elő.

Az Egyezmény 16. és 17. Cikke a tárolt számítástechnikai adatok, illetőleg a forgalomra vonatkozó adatok gyors megőrzésének jogintézményéről rendelkezik. A Be.-t átfogóan módosító 2002. évi I. törvény vezette be a Be. 158/A. §-ába új kényszerintézkedésként az Egyezmény rendelkezéseinek megfelelő, a számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés intézményét.

Az Egyezmény 18. Cikkében meghatározott közlésre kötelezés szabályaival összhangban a Be.-nek a megkeresésekre vonatkozó 71. §-ának szabályai lehetővé teszik az adatok közlését, illetőleg átadását is. A Be. 158. §-a szerint pedig az adatok megszerzésére irányuló kényszerintézkedéseket akadályozó személy az intézkedés tűrésére kényszeríthető, és a terhelt kivételével rendbírsággal sújtható.

Az Egyezmény 19. Cikke a tárolt számítástechnikai adatok lefoglalásának és átvizsgálásának a belső jogban történő szabályozását írja elő. Az említett Cikkel összhangban a Be. 149. §-a lehetővé teszi a számítástechnikai rendszer vagy az ilyen rendszer útján rögzített adatokat tartalmazó adathordozó átvizsgálását, míg a Be. 151. §-a biztosítja a számítástechnikai rendszer vagy az ilyen rendszer útján rögzített adatokat tartalmazó adathordozó lefoglalását.

Az Egyezmény 20. Cikke a forgalomra vonatkozó adatok valós idejű összegyűjtésének, míg 21. Cikke a tartalomra vonatkozó adatok kifürkészésének lehetővé tételét követeli meg a részes államoktól. A Be. 200. §-a (1) bekezdésének c) pontja biztosítja, hogy az ügyész és a nyomozó hatóság bírói engedély alapján az elkövető kilétének, tartózkodási helyének megállapítása, elfogása, valamint bizonyítási eszköz felderítése érdekében a nyomozás elrendelésétől a nyomozás iratainak ismertetéséig az érintett tudta nélkül a számítástechnikai rendszer útján továbbított és tárolt adatokat megismerhesse és felhasználhassa.

Az Egyezmény 22. Cikke szerint mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy megállapítsa joghatóságát az Egyezmény 2-11. Cikkében foglaltaknak megfelelően meghatározott bűncselekmények vonatkozásában, amennyiben a bűncselekményeket a területén; vagy a Fél lobogóját viselő hajó fedélzetén; vagy a Félnél lajstromozott repülőgép fedélzetén követték el, illetőleg amelyet a részes ország állampolgára követett el, ha a bűncselekmény az elkövetés helyének joga szerint büntetendő, vagy ha a bűncselekmény nem tartozik egyetlen állam joghatósága alá sem. A magyar Btk.

szabályozása teljes egészében megfelel az említett Cikkben meghatározott joghatósági szabályoknak.

A nemzetközi együttműködést szabályozó harmadik rész alapelvei között az Egyezmény rögzíti, hogy a szerződő felek a lehető legszélesebb körben együttműködnek a számítástechnikai rendszerrel kapcsolatos bűncselekmények alapján indult nyomozások és büntetőeljárások során, illetőleg az elektronikus formában megjelenő bizonyítékok összegyűjtése érdekében.

A magyar jog szabályai megfelelnek az Egyezmény kiadatásra és bűnügyi jogsegélyre vonatkozó rendelkezéseinek (24-28. Cikk).

Az Egyezmény 24. Cikke 7. bekezdésének a) pontja értelmében az aláírás, illetve a megerősítő, elfogadó, jóváhagyó vagy csatlakozó okmány letétbe helyezése alkalmával mindegyik Fél közli az Európa Tanács Főtitkárával valamennyi azon hatóság nevét és címét, amelynek hatáskörébe tartozik szerződés hiányában a kiadatási, illetve az ideiglenes kiadatási letartóztatásra irányuló kérelmek előterjesztése vagy fogadása.

A nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény (a továbbiakban: Nbjtv.) 18. §-a (1) bekezdésének értelmében a kiadatás iránti megkereséseket az igazságügy-miniszter fogadja, és a 26. § (1) bekezdése szerint dönt a kiadatás kérdésében is. A 33. § az igazságügy-miniszter jogkörébe utalja a kiadatási kérelem előterjesztéséről történő döntést is. Az Nbj.tv. 24. §-ának (2) bekezdése alapján az ideiglenes kiadatási letartóztatás iránti megkeresést az Országos Rendőr-főkapitányság Interpol Magyar Nemzeti Iroda útján is elő lehet terjeszteni. A fentebbi jogszabályhelyek rendelkezéseire figyelemmel a megerősítő okmány letétbe helyezésekor Magyarország az Egyezmény 24. Cikkével kapcsolatban azt a nyilatkozatot tette, hogy kiadatási szerződés hiányában a kiadatási kérelem, illetőleg az ideiglenes kiadatási letartóztatásra irányuló kérelem előterjesztésére vagy elfogadására az Igazságügyi Minisztérium jogosult. Az Interpol Magyar Nemzeti Iroda kizárólag az ideiglenes kiadatási letartóztatásra vonatkozó kérelmek előterjesztésére és fogadására jogosult.

Az Egyezmény 27. Cikke 2. bekezdésének a) és c) pontja értelmében a Szerződő Feleknek ki kell jelölniük, és az Európa Tanács Főtitkárával közölniük kell azokat a központi hatóságokat, amelyek hatályos nemzetközi megállapodások hiányában is jogosultak lesznek a jogsegély-kérelmek előterjesztésére, az azokra történő válaszadásra, azok teljesítésére vagy azoknak a teljesítés érdekében a hatáskörrel rendelkező hatóságokhoz történő megküldésére.

A megerősítő okmány letétbe helyezésekor Magyarország azt a nyilatkozatot tette, hogy az Egyezmény 27. Cikke 2. bekezdésének a) és c) pontja alapján a jogsegély-kérelmek előterjesztésére, az azokra történő válaszadásra, valamint azok teljesítésére vagy továbbküldésére jogosult központi hatóságként a büntetőeljárás megindítását megelőzően foganatosított megkeresések tekintetében az Országos Rendőr-főkapitányságon működő Nemzetközi Bűnügyi Együttműködési Központ (NEBEK), míg a büntetőeljárás megindítása után megküldött megkeresések tekintetében a Legfőbb Ügyészség jogosult.

Az Egyezmény 27. Cikke 9. bekezdésének a) pontja lehetővé teszi, hogy sürgős esetben a megkereső Fél igazságügyi hatóságai a jogsegélykérelmeket és az arra vonatkozó tájékoztatásokat közvetlenül a megkeresett Fél megfelelő igazságügyi hatóságaihoz intézhessék. A hivatkozott bekezdés e) pontja azonban biztosítja azt a lehetőséget, hogy az Egyezmény aláírása vagy a megerősítő, elfogadó, jóváhagyó vagy csatlakozási okmányok letétbe helyezése alkalmával bármely Szerződő Fél tájékoztathassa az Európa Tanács Főtitkárát, hogy célszerűségi okokból az említett bekezdés alapján előterjesztett kérelmeket központi hatóságához kell intézni.

Figyelemmel a hazai jogi szabályozásra, valamint az 1994. évi XIX. törvénnyel kihirdetett, Strasbourgban, 1959. április 20-án kelt, a kölcsönös bűnügyi jogsegélyről szóló európai egyezmény 15. cikk 6. bekezdéséhez fűzött fenntartásra, a megerősítő okmány letétbe helyezésekor Magyarország azt a nyilatkozatot tette, hogy az Egyezmény 27. Cikkének 9. bekezdése alapján, azaz sürgős esetben előterjesztett jogsegély-kérelmeket is a központi hatósághoz kell intézni.

A magyar jogi szabályozás lehetővé teszi, hogy az Egyezmény 29. és 30. Cikkeiben meghatározott ideiglenes intézkedéseket, valamint a 31-34. Cikkében szabályozott nyomozati cselekményeket a nemzetközi kapcsolatokban a magyar hatóságok jogsegély-kérelem alapján teljesítsék, illetőleg azok foganatosítása érdekében külföldi állam illetékes hatóságait megkeressék.

Az Egyezmény 35. Cikke kötelezi a Szerződő Feleket arra, hogy jelöljenek ki egy éjjel-nappal, a hét minden napján elérhető kapcsolattartási pontot, annak érdekében, hogy lehetővé tegyék a számítástechnikai adatokkal és rendszerrel összefüggő bűncselekményekre vonatkozó nyomozásokkal, vagy a bűncselekményekre vonatkozó elektronikus bizonyítékok összegyűjtésével kapcsolatos azonnali segítségnyújtást. Ez a segítségnyújtás lényegében az egyes nyomozati, illetőleg kényszercselekmények gyors foganatosításának megkönnyítését, elősegítését jelenti.

A Nemzetközi Bűnügyi Együttműködési Központ jogállásáról, részletes feladat- és hatásköréről, valamint a magyar bűnüldöző hatóságok és az Európai Rendőrségi Hivatal közötti nemzetközi együttműködésről szóló 4/2002. (I. 30.) BM-PM együttes rendelet 7. §-ának b) és d) pontja alapján a NEBEK feladata a külföldi bűnüldöző szervekkel bűnügyekben folytatott kapcsolattartás, együttműködés és információcsere, valamint az említett szervektől átvett megkeresések továbbítása a hatáskörrel rendelkező hazai bűnüldöző szervekhez.

Magyarország így a hét minden napján, éjjel-nappal elérhető kapcsolattartási pontként az Országos Rendőr-főkapitányságon működő Nemzetközi Bűnügyi Együttműködési Központot (NEBEK) jelölte ki, amelyről a megerősítő okmány letétbe helyezésekor az Egyezmény 35. Cikkéhez tett nyilatkozatában tájékoztatta az Európa Tanács Főtitkárát

4. Az Egyezményt 2001. november 23-án Budapesten nyitották meg aláírásra. Az Egyezmény az Európa Tanács történetében az első „Budapesti Egyezmény”, egyben a számítástechnikai bűnözés elleni fellépés tárgykörében született első nemzetközi szerződés.

A tárgykör fontosságának megfelelően már az aláírásra történt megnyitáskor - az Európa Tanács történetében kiemelkedően magas számú résztvevő - 30 ország írta alá. Az Egyezmény ún. nyitott egyezmény, azaz a csatlakozás, aláírás lehetősége a nem Európa Tanács-i tagállamok számára is nyitva áll. Ennek megfelelően az Egyezmény szövegezésében a tagállamok mellett részt vett az Amerikai Egyesült Államok, Kanada, Japán és a Dél-Afrikai Köztársaság is, amely országok már Budapesten aláírták az Egyezményt.

5. Az Egyezményt a 2337/2001. (XI. 22.) Korm. határozat alapján a Magyar Köztársaság képviseletében az igazságügy-miniszter 2001. november 23-án írta alá az országgyűlési megerősítés fenntartásával.

A Magyar Köztársaság Országgyűlése 2002. november 12-i ülésén elfogadott 82/2002. (XI. 13.) OGY határozatával erősítette meg az Egyezményt. A megerősítő okmány letétbe helyezése az Európa Tanács Főtitkáránál 2003. december 4-én megtörtént.

6. Az Egyezmény hatályba lépésének feltétele, hogy öt aláíró állam, közülük legalább három az Európa Tanács tagja, az Európa Tanács Főtitkáránál letétbe helyezze a megerősítő, elfogadási vagy jóváhagyási okmányokat. Albánia, Horvátország, Észtország, és Magyarország után 2004. március 18-án Litvánia is letétbe helyezte megerősítő okmányát. Az Egyezmény így 2004. július 1-jén hatályba lép, rendelkezéseit ezen időponttól kell alkalmazni.

7. Figyelemmel a jogalkotásról szóló 1987. évi XI. törvény 2. §-ának c) pontjában, valamint a nemzetközi szerződésekkel kapcsolatos eljárásról szóló 1982. évi 27. törvényerejű rendelet 13. §-ának (1) bekezdésében foglaltakra, az Egyezményt törvénnyel szükséges kihirdetni.

## Részletes Indokolás

### Az 1-2. §-hoz

A Javaslat 1. §-a rendelkezik az Egyezmény kihirdetéséről, a 2. § tartalmazza az Egyezmény hiteles angol nyelvű szövegét és annak hivatalos magyar nyelvű fordítását.

### A 3. §-hoz

A Javaslat 3. §-ának (1) bekezdése tartalmazza az Egyezmény megerősítéséről szóló okirat letétbe helyezésekor, az Országgyűlés felhatalmazása alapján, a Magyar Köztársaság Kormánya által tett fenntartást.

A Javaslat 3. §-ának (2) bekezdése tartalmazza az Egyezmény megerősítéséről szóló okirat letétbe helyezésekor, az Országgyűlés felhatalmazása alapján, a Magyar Köztársaság Kormánya által tett nyilatkozatokat.

**A 4. §-hoz**

A Javaslat 4. §-a rendelkezik a törvény hatályba lépésének időpontjáról, valamint arról, hogy az Egyezmény nemzetközi hatályba lépésére figyelemmel rendelkezéseit mely időponttól kell alkalmazni.