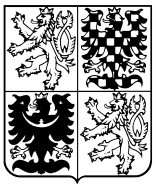
Ročník 2013



SBÍRKA MEZINÁRODNÍCH SMLUV

ČESKÁ REPUBLIKA

Částka 56 **Rozeslána dne 23. prosince 2013** **Cena Kč 128,–**

OBSAH:

104

SDĚLENÍ

Ministerstva zahraničních věcí

Ministerstvo zahraničních věcí sděluje, že dne 23. listopadu 2001 byla v Budapešti otevřena k podpisu Úmluva o počítačové kriminalitě.

Jménem České republiky byla Úmluva podepsána ve Štrasburku dne 9. února 2005.

S Úmluvou vyslovil souhlas Parlament České republiky a prezident republiky ji ratifikoval. Ratifikační listina České republiky byla uložena u generálního tajemníka Rady Evropy, depozitáře Úmluvy, dne 22. srpna 2013.

Při ratifikaci Úmluvy byla učiněna následující výhrada České republiky:

„V souladu s článkem 29 odst. 4 a článkem 42 Úmluvy o počítačové kriminalitě Česká republika prohlašuje, že si vyhrazuje právo odmítnout žádost o uchování podle článku 29 Úmluvy v případech, kdy lze předpokládat, že by nebylo možno, ve vztahu k trestným činům jiným, než jsou ty, stanovené podle článků 2 až 11 Úmluvy, naplnit podmínku oboustranné trestnosti pro vyřízení žádosti o vzájemnou pomoc týkající se prohlídky nebo podobného přístupu, zajištění nebo podobného zabezpečení, nebo zpřístupnění uložených dat.“

Současně bylo učiněno toto prohlášení:

„V souladu s článkem 2 a článkem 40 Úmluvy o počítačové kriminalitě Česká republika prohlašuje, že trestní odpovědnost za jednání popsané v článku 2 této Úmluvy vzniká překonáním bezpečnostního opatření za účelem získání neoprávněného přístupu k počítačovému systému nebo jeho části.

V souladu s článkem 27 odst. 9 písm. e) Úmluvy o počítačové kriminalitě Česká republika prohlašuje, že z důvodů efektivity mají být žádosti podle tohoto odstavce adresovány ústředním orgánům.“

Při uložení listiny o přístupu bylo rovněž učiněno následující oznámení:

„V souladu s článkem 24 odst. 7 písm. a) Úmluvy o počítačové kriminalitě Česká republika prohlašuje, že v případě neexistence smlouvy o vydávání bude orgánem odpovědným za předkládání nebo přijímání žádostí o vydání nebo o předběžnou vazbu Ministerstvo spravedlnosti České republiky (Vyšehradská 16, 128 10 Praha 2).

V souladu s článkem 27 odst. 2 písm. a) Úmluvy o počítačové kriminalitě Česká republika prohlašuje, že ústředním orgánem, který je zodpovědný za předkládání žádostí a odpovídání na žádosti o vzájemnou pomoc, vyřizování takových žádostí nebo jejich předávání orgánům příslušným pro jejich vyřizování, je Nejvyšší státní zastupitelství České republiky pro žádosti vzešlé z přípravného řízení a Ministerstvo spravedlnosti České republiky pro ostatní žádosti.

Adresy ústředních orgánů určených v souladu s ustanovením článku 27 odst. 2 písm. a) této Úmluvy:

Nejvyšší státní zastupitelství České republiky
Jezuitská 4
660 55 Brno
Česká republika
Telefon: +420 542 512 330
Fax: +420 542 512 350
E-mail: podatelna@nsz.brn.justice.cz

Ministerstvo spravedlnosti České republiky
Vyšehradská 16
128 10 Praha 2
Česká republika
Telefon: +420 221 997 435
Fax: +420 221 997 986
E-mail: mot@msp.justice.cz

V souladu s článkem 35 Úmluvy o počítačové kriminalitě Česká republika oznamuje, že jako kontaktní místo je určeno:

Policejní prezidium České republiky
Úřad služby kriminální policie a vyšetřování
Odbor informační kriminality
Strojnická 27
P.O.Box 62/KPV
170 89 Praha 7
Česká republika

Kontakt v pracovní době (7:30 – 15:30):
Telefon: +420 974 834 550
Mobil: +420 603 190 057
Fax: +420 974 834 708
E-mail: contact@mvcr.cz

Kontakt mimo pracovní dobu (služba 24/7):
Telefon: +420 974 834 380
Fax: +420 974 834 716
E-mail: contact@mvcr.cz“.

Úmluva vstoupila v platnost na základě svého článku 36 odst. 3 dne 1. července 2004. Pro Českou republiku vstoupila v platnost podle odstavce 4 téhož článku dne 1. prosince 2013.

Anglické znění Úmluvy a její překlad do českého jazyka se vyhlašují současně.

CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001

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 – Offencesrelated 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 – Procedurallaw

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 – Internationalco-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 – Principlesrelating 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 assistanæ 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 ob jectives 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.

PŘEKLAD

Úmluva o počítačové kriminalitě

Preambule

Členské státy Rady Evropy a ostatní státy, které podepsaly tuto Úmluvu,

majíce na zřeteli, že cílem Rady Evropy je dosáhnout větší jednoty mezi jejími členy,

uznávajíce hodnotu budování spolupráce s ostatními státy, které podepsaly tuto Úmluvu,

jsouce přesvědčeny o potřebě prioritního uskutečňování společné trestní politiky zaměřené na ochranu společnosti proti počítačové kriminalitě, *zvláště pak* přijetím příslušných právních předpisů a budováním mezinárodní spolupráce,

při vědomí zásadních změn způsobených digitalizací, konvergencí a pokračující globalizací počítačových sítí,

jsouce znepokojeny rizikem, že počítačové sítě a elektronické informace mohou být také zneužity pro páchání trestných činů a že důkazy o těchto trestných činech mohou být uchovávány v těchto sítích a prostřednictvím těchto sítí přenášeny,

uznávajíce potřebu spolupráce mezi státy a soukromými podnikateli při potírání počítačové kriminality a potřebu chránit legitimní zájmy při používání a rozvoji informačních technologií,

věříce, že účinný boj proti počítačové kriminalitě vyžaduje zvýšenou, urychlenou a funkční mezinárodní spolupráci v trestních věcech,

jsouce přesvědčeny, že tato Úmluva je nezbytná pro odrazení od činů namířených proti důvěrnosti, integritě a dostupnosti počítačových systémů, sítí a počítačových dat, i proti zneužití těchto systémů, sítí a dat tím, že stanoví kriminalizaci takového chování, jak je popsáno v této Úmluvě, a přijetí pravomocí dostatečných pro účinné potírání takových trestných činů tím, že usnadňuje zjišťování, vyšetřování a trestní stíhání takových trestných činů na vnitrostátní i mezinárodní úrovni a stanoví mechanismy pro rychlou a spolehlivou mezinárodní spolupráci,

majíce na paměti potřebu zajistit správnou rovnováhu mezi zájmy vynucování práva a respektováním základních lidských práv, jak jsou zakotvena v Úmluvě Rady Evropy o ochraně lidských práv a základních svobod z roku 1950, Mezinárodním Paktu Organizace spojených národů o občanských a politických právech z roku 1966, jakož i ostatních příslušných mezinárodních úmluv o lidských právech, které opětovně stvrzují právo každého jednotlivce na zastávání názorů bez postihu i právo na svobodu projevu, včetně svobody vyhledávat, získávat a sdělovat informace i myšlenky všeho druhu, bez ohledu na hranice, a dále pak práva týkající se respektu k soukromí,

majíce také na paměti ochranu osobních údajů, jak je stanovena například v Úmluvě Rady Evropy o ochraně jednotlivců při automatickém zpracování osobních údajů z roku 1981,

majíce na zřeteli Úmluvu Organizace spojených národů o právech dětí z roku 1989 a Úmluvu Mezinárodní organizace práce o nejhorších formách dětské práce z roku 1999,

berouce v úvahu stávající úmluvy Rady Evropy o spolupráci v oblasti trestního práva i podobné smlouvy, které existují mezi členskými státy Rady Evropy a jinými státy a s důrazem na to, že tato Úmluvy je zamýšlena k doplnění těchto úmluv tak, aby bylo možno účinněji provádět trestní vyšetřování i řízení týkající se trestných činů spojených s počítačovými systémy a daty a umožnit shromažďování elektronických důkazů trestného činu,

vítajíce poslední vývoj, který dále posiluje mezinárodní porozumění i spolupráci v boji proti počítačovým trestným činům, včetně aktivit Organizace spojených národů, OECD, Evropské Unie a G8,

dovolávajíce se Doporučení č. R (85) 10 o praktickém provádění Evropské Úmluvy o vzájemné pomoci v trestních věcech v souvislosti s dožádáními týkajícími se odposlechu telekomunikací, Doporučení č. R (88) 2 o pirátství v oblasti autorských a přidružených práv, Doporučení č. R (87) 15 upravující použití osobních dat v policejním sektoru, Doporučení č. R (95) 4 o ochraně osobních dat v oblasti telekomunikačních služeb, se zvláštním ohledem na telefonní služby i Doporučení č. R (89) 9 o kriminalitě spojené s počítači, stanovící směrnice pro národní zákonodárce ohledně definování určitých počítačových trestných činů a Doporučení č. R (95) 13 o problémech trestního procesního práva spojených s informační technologií,

vzhledem k Rezoluci č. 1 přijatou evropskými ministry spravedlnosti na jejich 21. konferenci (Praha, červen 1997), která doporučila Výboru ministrů podporovat práci Evropského výboru pro problémy kriminality (CDPC) v oblasti počítačové kriminality s cílem sbližovat vnitrostátní ustanovení trestního práva a umožňovat použití účinných prostředků vyšetřování takových trestných činů, a rovněž s ohledem na Rezoluci č. 3 přijatou na 23. konferenci evropských ministrů spravedlnosti (Londýn, červen 2000), která vyzvala jednající strany k pokračování jejich úsilí o nalezení vhodných řešení, aby se co nejvíce států mohlo stát stranami Úmluvy a stvrdila potřebu rychlého a účinného systému mezinárodní spolupráce, který bude brát náležitě v potaz specifické požadavky boje proti počítačové kriminalitě,

dále pak s ohledem na Plán činnosti schválený hlavami států a vlád Rady Evropy u příležitosti jejich druhého summitu (Štrasburk, 10. – 11. října 1997) o hledání společných odpovědí na vývoj nových informačních technologií, které budou založeny na standardech a hodnotách Rady Evropy,

se dohodly na následujícím:

Kapitola I – Užití pojmů

Článek 1 - Definice

Pro účely této Úmluvy:

a. "počítačový systém" znamená jakékoli zařízení nebo skupinu propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu;

b. "počítačová data" znamenají jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem;

c. "poskytovatel služby" znamená:

(i) jakýkoli veřejný nebo soukromý subjekt, který uživatelům své služby umožňuje komunikovat prostřednictvím počítačového systému, a

(ii) jakýkoli jiný subjekt, který zpracovává nebo uchovává počítačová data pro takovou komunikační službu nebo pro uživatele takové služby.

d. "provozní data" znamenají jakákoli počítačová data vztahující se ke komunikaci prostřednictvím počítačového systému, vytvořená počítačovým systémem, jakožto součástí komunikačního řetězce, uvádějící původ, cíl, cestu, čas, datum, objem nebo trvání komunikace nebo typ příslušné služby.

Kapitola II – Opatření, která mají být přijata na vnitrostátní úrovni

Část 1 – Trestní právo hmotné

Oddíl 1 – Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů

Článek 2 – Nezákonný přístup

Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byl trestným činem, pokud je spáchán úmyslně, neoprávněný přístup k celému počítačovému systému nebo jeho jakékoli části. Strana může stanovit, že bude považovat tento čin za trestný, jen pokud je spáchán porušením bezpečnostních opatření, s úmyslem získat počítačová data nebo s jiným nečestným úmyslem, nebo ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem.

Článek 3 – Nezákonný odposlech

Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byl trestným činem úmyslný, neoprávněný, technickými prostředky provedený odposlech neveřejného přenosu

počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému přenášejícího taková počítačová data. Strana může stanovit, že bude považovat tento čin za trestný, jen pokud je spáchán s nečestným úmyslem, nebo ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem.

Článek 4 – Zasahování do dat

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně, neoprávněné poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat.

2. Strana si může vyhradit právo stanovit, že bude považovat jednání popsané v odstavci 1 za trestné, jen pokud způsobí závažnou škodu.

Článek 5 – Zasahování do systému

Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně, neoprávněné závažné omezení funkčnosti počítačového systému vkládáním, přenášením, poškozením, vymazáním, snížením kvality, pozměněním nebo potlačením počítačových dat.

Článek 6 – Zneužívání zařízení

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byly trestnými činy, pokud jsou spáchány úmyslně a neoprávněně:

   (a) výroba, prodej, opatření za účelem použití, dovoz, distribuce nebo jiné zpřístupnění:

      i. zařízení, včetně počítačového programu, vytvořeného nebo přizpůsobeného zejména za účelem spáchání kteréhokoli z trestných činů stanovených podle článků 2 – 5;

      ii. počítačového hesla, přístupového kódu nebo podobných dat, pomocí nichž lze získat přístup do celého počítačového systému nebo do jakékoli jeho části

   s tím úmyslem, že jej bude použito pro účely spáchání kteréhokoli z trestných činů stanovených podle článků 2 až 5; a

   (b) držení jedné z položek uvedených v odstavcích (a) i. nebo (a) ii. shora s tím úmyslem, že bude použita pro účely spáchání kteréhokoli z trestných činů stanovených v článcích 2 až 5. Strana může zákonem stanovit, že trestní odpovědnost vzniká až při držení několika takových položek.

2. Tento článek nelze vykládat tak, že stanoví trestní odpovědnost v případech, kdy nejde o výrobu, prodej, opatření za účelem použití, dovoz, distribuci nebo jiné zpřístupnění nebo držení uvedené v odstavci 1 tohoto článku za účelem spáchání trestného činu stanoveného podle článků 2 až 5 této Úmluvy, jako třeba při oprávněném zkoušení nebo ochraně počítačového systému.

3. Každá strana si může vyhradit právo nepoužít odstavec 1 tohoto článku za podmínky, že se tato výhrada nebude týkat prodeje, distribuce nebo jiného zpřístupnění předmětů uvedených v odstavci 1(a) ii.

Oddíl 2 – Trestné činy související s počítačem

Článek 7 – Počítačové padělání

Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byly trestnými činy, pokud jsou spáchány úmyslně a neoprávněně, vkládání, pozměnění, vymazání nebo potlačení počítačových dat, které povede k nepravosti dat, a to s úmyslem, aby tato data byla považována za pravá nebo aby podle nich bylo pro právní účely jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná či nikoli. Strana může stanovit, že k založení trestní odpovědnosti je nezbytný úmysl podvést nebo podobný nečestný úmysl.

Článek 8 – Počítačový podvod

Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně a neoprávněně, způsobení ztráty na majetku jinému:

(a) jakýmkoli vkládáním, pozměňováním, vymazáním nebo potlačením počítačových dat,

(b) jakýmkoli zásahem do fungování počítačového systému,

s podvodným nebo nečestným úmyslem neoprávněně získat majetkový prospěch pro sebe nebo pro jiného.

Oddíl 3 – Trestné činy související s obsahem

Článek 9 – Trestné činy související s dětskou pornografií

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně a neoprávněně, následující jednání:

(a) výroba dětské pornografie za účelem její distribuce prostřednictvím počítačového systému;

(b) nabízení nebo zpřístupňování dětské pornografie prostřednictvím počítačového systému;

(c) distribuce nebo přenos dětské pornografie prostřednictvím počítačového systému;

(d) opatřování dětské pornografie prostřednictvím počítačového systému pro sebe nebo pro jiného;

(e) uchovávání dětské pornografie v počítačovém systému nebo na médiu pro ukládání počítačových dat.

2. Pro účely výše uvedeného odstavce 1 "dětská pornografie" bude zahrnovat pornografický materiál, který vizuálně znázorňuje:

(a) nezletilou osobu, která se účastní sexuálně jednoznačného chování;

(b) osobu, jež se zdá být nezletilou, která se účastní sexuálně jednoznačného chování;

(c) realistické zobrazení představující nezletilou osobu, která se účastní sexuálně jednoznačného chování.

3. Pro účely odstavce 2 shora bude termín "nezletilý" zahrnovat všechny osoby mladší 18 let. Strana však může stanovit nižší věkovou hranici, která ale nesmí být nižší než 16 let.

4. Každá strana si může vyhradit právo nepoužít vcelku nebo zčásti odstavce 1 (d) a 1 (e), a 2 (b) a 2 (c).

Oddíl 4 – Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským

Článek 10 - Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem porušení autorského práva, jak je definováno právními předpisy této strany podle závazků, které přijala na základě Pařížské revize z 24. července 1971 Bernské Úmluvy o ochraně literárních a uměleckých děl, Dohody o obchodních aspektech práv k duševnímu vlastnictví a Smlouvy Světové organizace duševního vlastnictví (WIPO) o právu autorském, s výjimkou jakýchkoli osobnostních práv stanovených těmito úmluvami, pokud jsou tyto činy spáchány záměrně, v komerčním měřítku a prostřednictvím počítačového systému.

2. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem porušení práv souvisejících s právem autorským, jak jsou definována právními předpisy této strany podle závazků, které přijala na základě Mezinárodní úmluvy o ochraně výkonných umělců, výrobců zvukových snímků a rozhlasových organizací (Římská úmluva), Dohody o obchodních aspektech práv k duševnímu vlastnictví a Smlouvy WIPO o výkonech výkonných umělců a o zvukových záznamech, s výjimkou jakýchkoli osobnostních práv

stanovených těmito úmluvami, pokud jsou tyto činy spáchány záměrně, v komerčním měřítku a prostřednictvím počítačového systému.

3. Strana si může vyhradit právo nestanovit trestní odpovědnost podle odstavců 1 a 2 tohoto článku v omezeném rozsahu okolností, pokud jsou dostupná jiná účinná nápravná opatření a pokud tato výhrada neomezuje mezinárodní závazky strany stanovené v mezinárodních dokumentech uvedených v odstavcích 1 a 2 tohoto článku.

Oddíl 5 – Další formy odpovědnosti a trestů

Článek 11 – Pokus trestného činu a účastenství

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byla trestným činem, jakákoli úmyslná forma účastenství na spáchání kteréhokoli trestného činu podle článků 2 až 10 této Úmluvy, s tím úmyslem, aby takový trestný čin byl spáchán.

2. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byl trestným činem úmyslný a neoprávněný pokus spáchat jakýkoli trestný čin podle článků 3 až 5, 7, 8, 9 (1) a) a 9 (1) c) této Úmluvy.

3. Každý stát si může vyhradit právo nepoužít odstavec 2 tohoto článku nebo jeho část.

Článek 12 – Odpovědnost právnických osob

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby zajistila, že právnická osoba může být učiněna odpovědnou za trestný čin ustavený podle této Úmluvy, spáchaný v její prospěch jakoukoli fyzickou osobou, která v ní má vedoucí postavení, ať již jedná samostatně nebo jako člen orgánu této právnické osoby, na základě:

   (a) pravomoci jednat navenek jménem právnické osoby;

   (b) pravomoci přijímat rozhodnutí jménem právnické osoby;

   (c) pravomoci vykonávat kontrolu v rámci právnické osoby.

2. Kromě případů, na něž se již vztahují ustanovení v odstavci 1, podnikne každá strana nezbytná opatření pro zajištění toho, že právnická osoba může být uznána odpovědnou v případech, kdy nedostatek dohledu nebo kontroly ze strany fyzické osoby zmíněné v odstavci 1 umožnil spáchání trestného činu, ustaveného v souladu s touto Úmluvou, ve prospěch této právnické osoby fyzickou osobou jednající v rámci její pravomoci.

3. Podle právních principů strany může být odpovědnost právnické osoby trestní, občanskoprávní nebo správní.

4. Tato odpovědnost nebude mít vliv na trestní odpovědnost fyzických osob, které trestný čin spáchaly.

Článek 13 – Tresty a opatření

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby trestné činy ustavené podle článků 2-11 bylo možno potrestat účinnými, přiměřenými a odrazujícími tresty, včetně trestu odnětí svobody.

2. Každá strana zajistí, aby právnické osoby uznané odpovědnými podle článku 12 podléhaly účinným, přiměřeným a odrazujícím trestním nebo netrestním sankcím nebo opatřením, včetně peněžitých sankcí.

Část 2 – Procesní právo

Oddíl 1 – Obecná ustanovení

Článek 14 - Rozsah procesních ustanovení

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby zavedla pravomoci a postupy stanovené v této části pro účely specifických trestních vyšetřování nebo řízení.

2. Pokud není upraveno jinak v článku 21, každá strana použije pravomoci a postupy uvedené v odstavci 1:

   (a) na trestné činy stanovené podle článků 2 až 11 této Úmluvy;

   (b) na jiné trestné činy spáchané prostřednictvím počítačového systému; a

   (c) na zajištění důkazů o trestném činu, které jsou v elektronické formě.

3. (a) Každá strana si může vyhradit právo použít opatření uvedená v článku 20 pouze na trestné činy nebo kategorie trestných činů uvedené ve výhradě, pokud okruh takových trestných činů nebo kategorií trestných činů není více omezený než okruh trestných činů, na které strana používá opatření uvedená v článku 21. Každá strana zváží omezení takové výhrady, aby umožnila co nejširší používání opatření uvedeného v článku 20.

   (b) Pokud strana není, kvůli omezením ve svých právních předpisech platných v době přijetí této Úmluvy, schopna použít opatření uvedená v článcích 20 a 21 na komunikace přenášené v rámci počítačového systému poskytovatele služeb, který

      (i) je provozovaný pro potřeby uzavřené skupiny uživatelů, a

      (ii) nepoužívá veřejné komunikační sítě a není propojen s jiným počítačovým systémem, ať již veřejným nebo soukromým,

   tato strana si může vyhradit právo nepoužít tato opatření na takové komunikace. Každá strana zváží omezení takové výhrady, aby umožnila co nejširší používání opatření uvedených v článcích 20 a 21.

Článek 15 – Podmínky a záruky

1. Každá strana zajistí, že založení, implementace a používání pravomocí a postupů stanovených v této části podléhá podmínkám a zárukám stanoveným podle jejích vnitrostátních právních předpisů, které poskytnou přiměřenou ochranu lidských práv a svobod, včetně práv vyplývajících ze závazků, které převzala podle Úmluvy Rady Evropy na ochranu lidských práv a základních svobod z roku 1950, Mezinárodního paktu OSN o občanských a politických právech z roku 1966, a dalších příslušných mezinárodních dokumentů o lidských právech, a které budou obsahovat princip přiměřenosti.

2. Takové podmínky a záruky budou, přiměřeně s ohledem na povahu příslušné pravomoci nebo postupu, zahrnovat mimo jiné soudní nebo jiný nezávislý dohled, důvody opravňující použití, a omezení rozsahu a trvání takové pravomoci nebo postupu.

3. Strany zváží dopad pravomocí a postupů v této části na práva, odpovědnosti a legitimní zájmy třetích stran v mezích, které jsou slučitelné s veřejným zájmem, zejména s řádným výkonem spravedlnosti.

Oddíl 2 - Urychlené uchování uložených počítačových dat

Článek 16 – Urychlené uchování uložených počítačových dat

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby umožnila svým příslušným orgánům přikázat anebo obdobně zajistit urychlené uchování specifických počítačových dat, včetně provozních dat, které byly uloženy prostřednictvím počítačového systému, zejména pokud existují důvody pro přesvědčení, že tato počítačová data jsou zvláště ohrožená ztrátou nebo pozměněním.

2. V případech, kdy strana uplatňuje ustanovení výše uvedeného odstavce 1 pomocí příkazu určité osobě, aby zachovala specifikovaná uložená počítačová data v držení této osoby nebo pod její kontrolou, tato strana přijme taková legislativní a jiná opatření, která mohou být nezbytná pro uložení povinnosti této osobě, aby zachovala a udržovala neporušenost takových počítačových dat po nezbytné období, nejvýše po 90 dnů, aby mohly příslušné orgány požádat o jejich zpřístupnění. Strana může umožnit následné obnovení takového příkazu.

3. Každá strana přijme taková legislativní nebo jiná opatření, která budou nezbytná k tomu, aby uložila správci nebo jiné osobě, která má uchovat počítačová data, povinnost udržovat přijímání takových postupů v tajnosti po dobu stanovenou svými vnitrostátními právními předpisy.

4. Pravomoci a postupy uvedené v tomto článku budou podléhat článkům 14 a 15.

Článek 17 – Urychlené zachování a urychlené částečné zpřístupnění provozních dat

1. Každá strana přijme ve vztahu k provozním datům, která mají být zachována podle článku 16, taková legislativní a jiná opatření, která budou nezbytná pro:

(a) zajištění, že takové urychlené zachování provozních dat je použitelné bez ohledu na to, zda se přenosu dané komunikace účastnil jeden nebo více poskytovatelů služeb; a

(b) zajištění toho, že příslušnému orgánu strany nebo osobě určené tímto orgánem bude urychleně zpřístupněno množství provozních dat dostatečné k tomu, aby strana mohla identifikovat poskytovatele služeb a cestu, kterou byla komunikace přenesena.

2. Pravomoci a postupy uvedené v tomto článku budou podléhat článkům 14 a 15.

Oddíl 3 – Příkaz k předložení

Článek 18 – Příkaz k předložení

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby umožnila svým příslušným orgánům nařídit:

(a) osobě na svém území, aby předložila specifikovaná počítačová data v jejím držení nebo pod její kontrolou, která jsou uložena v počítačovém systému nebo na médiu pro ukládání počítačových dat; a

(b) poskytovateli služby nabízejícímu své služby na území strany, aby předložil ty informace o odběrateli vztahující se k těmto službám, které jsou v jeho držení nebo pod jeho kontrolou.

2. Pravomoci a postupy uvedené v tomto článku budou podléhat článkům 14 a 15.

3. Pro účely tohoto článku znamená „informace o odběrateli" jakoukoli informaci, obsaženou ve formě počítačových dat nebo jakékoli jiné formě, odlišnou od provozních nebo obsahových dat, která je držena poskytovatelem služeb, vztahuje se k účastníkům jeho služeb, a s jejíž pomocí lze určit:

(a) typ použité komunikační služby, za tím účelem provedená technická opatření a období služby;

(b) identitu odběratele, poštovní nebo geografickou adresu, telefonní a jiné přístupové číslo, účetní a platební informace, dostupné na základě dohody nebo ujednání o poskytování služeb;

(c) jakoukoli jinou informaci o místě instalace komunikačního vybavení dostupnou na základě dohody nebo ujednání o poskytování služeb.

Oddíl 4 – Prohlídka a zajištění uložených počítačových dat

Článek 19 - Prohlídka a zajištění uložených počítačových dat

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby umožnila svým příslušným orgánům prohledat nebo podobným způsobem získat přístup:

   (a) k počítačovému systému nebo jeho části a k počítačovým datům v něm uloženým; a

   (b) k médiu pro ukládání počítačových dat, na kterém mohou být uložena počítačová data,

   na svém území.

2. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby zajistila, že pokud její orgány prohledají nebo podobným způsobem získají přístup ke konkrétnímu počítačovému systému nebo jeho části podle odstavce 1 (a) a mají důvod k přesvědčení, že hledaná data jsou uložena v jiném počítačovém systému nebo jeho části na jejím území a že tato data jsou legálně přístupná z původního systému nebo jsou mu k dispozici, tyto orgány budou moci urychleně rozšířit prohlídku nebo podobným způsobem získat přístup k tomuto druhému systému.

3. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby umožnila svým příslušným orgánům zajistit nebo podobně zabezpečit počítačová data, k nimž byl zjednán přístup podle odstavců 1 nebo 2. Tato opatření budou zahrnovat pravomoc:

   (a) zajistit nebo podobně zabezpečit počítačový systém, jeho část nebo médium pro ukládání počítačových dat;

   (b) pořídit a uchovat kopii takových počítačových dat;

   (c) uchovat neporušenost relevantních uložených počítačových dat; a

   (d) znemožnit přístup k takovým počítačovým datům nebo je odstranit z počítačového systému, k němuž byl zjednán přístup.

4. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby umožnila svým příslušným orgánům přikázat kterékoli osobě, která má znalosti o fungování počítačového systému nebo o opatřeních použitých na ochranu počítačových dat v tomto systému, aby poskytla nezbytné informace v přiměřeném rozsahu pro umožnění realizace opatření uvedených v odstavcích 1 a 2.

5. Pravomoci a postupy uvedené v tomto článku budou podléhat článkům 14 a 15.

Oddíl 5 – Shromažďování počítačových dat v reálném čase

Článek 20 – Shromažďování provozních dat v reálném čase

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby svým příslušným orgánům umožnila:

   (a) provádět pomocí technických prostředků na území této strany shromažďování nebo záznam; a

   (b) přinutit poskytovatele služeb, aby v rámci svých stávajících technických možností:

      i. pomocí technických prostředků na území této strany prováděl shromažďování nebo zaznamenávání; nebo
      ii. spolupracoval a napomáhal příslušným orgánům při shromažďování nebo zaznamenávání

   provozních dat, v reálném čase, spojených s určenými komunikacemi na jejím území přenášenými pomocí počítačového systému.

2. Pokud strana z důvodu zavedených principů svého vnitrostátního právního řádu nemůže přijmout opatření uvedené v odstavci 1(a), může místo toho přijmout legislativní a jiná opatření, která budou nezbytná k tomu, aby zajistila shromažďování nebo záznam provozních dat v reálném čase, spojených se specifikovanými komunikacemi na jejím území za použití technických prostředků na tomto území.

3. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby uložila poskytovateli služeb povinnost zachovat v důvěrnosti výkon jakékoli pravomoci stanovené tímto článkem i jakoukoli jinou informaci o něm.

4. Pravomoci a postupy uvedené v tomto článku budou podléhat článkům 14 a 15.

Článek 21 – Odposlech obsahových dat

1. Každá strana přijme ve vztahu k okruhu závažných trestných činů, který bude stanoven vnitrostátními právními předpisy, taková legislativní a jiná opatření, která budou nezbytná k tomu, aby umožnila svým příslušným orgánům:

   (a) provádět pomocí technických prostředků na území této strany shromažďování nebo záznam; a

   (b) přinutit poskytovatele služeb, aby v rámci svých stávajících technických možností:

      i. prováděl pomocí technických prostředků na území této strany shromažďování nebo záznam; nebo

      ii. spolupracoval a napomáhal příslušným orgánům při shromažďování a zaznamenávání

obsahových dat, v reálném čase, určených komunikací na jejím území přenášených pomocí počítačového systému.

2. Pokud strana z důvodu zavedených principů svého vnitrostátního právního řádu nemůže přijmout opatření uvedené v odstavci 1(a), může místo toho přijmout legislativní a jiná opatření, která budou nezbytná k tomu, aby zajistila shromažďování nebo záznam, v reálném čase, obsahových dat specifikovaných komunikací na jejím území za použití technických prostředků na tomto území.

3. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby uložila poskytovateli služeb povinnost zachovat v důvěrnosti výkon jakékoli pravomoci stanovené tímto článkem i jakoukoli jinou informaci o něm.

4. Pravomoci a postupy uvedené v tomto článku budou podléhat článkům 14 a 15.

Část 3 – Soudní pravomoc

Článek 22 – Soudní pravomoc

1. Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby stanovila svou soudní pravomoc ve vztahu k jakémukoli trestnému činu podle článků 2 až 11 této Úmluvy, pokud je trestný čin spáchán:

   (a) na jejím území; nebo

   (b) na lodi plující pod vlajkou této strany; nebo

   (c) na palubě letadla registrovaného podle zákonů této strany; nebo

   (d) jedním z jejích státních příslušníků, pokud je tento čin trestný podle trestního práva v místě, kde byl spáchán, nebo pokud byl tento čin spáchán na území, na něž se nevztahuje územní pravomoc žádného státu.

2. Každý stát si může vyhradit právo nepoužít nebo použít pouze ve specifických případech nebo okolnostech pravidla pro soudní pravomoc uvedená v odstavcích 1 (b) – 1 (d) tohoto článku nebo jejich jakékoli části.

3. Každá strana přijme taková opatření, která budou nezbytná k tomu, aby stanovila svou soudní pravomoc ve vztahu k trestným činům uvedeným v článku 24, odstavci (1) této Úmluvy v případech, kdy se údajný pachatel nachází na jejím území a tato strana jej nevydá jiné straně výlučně na základě jeho státní příslušnosti, a to po žádosti o vydání.

4. Tato Úmluva nevylučuje žádnou trestní soudní pravomoc vykonávanou v souladu s vnitrostátními právními předpisy.

5. Pokud více než jedna strana nárokuje pravomoc vůči údajnému trestnému činu podle této Úmluvy, zúčastněné strany se, pokud to bude vhodné, vzájemně poradí, aby určily nejvhodnější pravomoc pro trestní stíhání.

Kapitola III – Mezinárodní spolupráce

Část 1 – Obecné zásady

Oddíl 1 – Obecné zásady týkající se mezinárodní spolupráce

Článek 23 - Obecné zásady týkající se mezinárodní spolupráce

Strany budou vzájemně spolupracovat podle ustanovení této kapitoly a na základě uplatňování příslušných mezinárodních dokumentů o mezinárodní spolupráci v trestních věcech, podle ujednání dohodnutých na základě jednotných právních předpisů, reciproční právní úpravy a vnitrostátních zákonů, v nejširší možné míře pro účely vyšetřování nebo řízení týkající se trestných činů vztahujících se na počítačové systémy a data, nebo pro shromažďování důkazů v elektronické formě o trestném činu.

Oddíl 2 – Zásady týkající se vydávání

Článek 24 - Vydávání osob

1. (a) Tento článek se vztahuje na vydávání osob mezi stranami pro trestné činy stanovené v článcích 2 - 11 této Úmluvy, pokud podléhají podle práva obou zúčastněných stran trestu odnětí svobody, jehož horní hranice je nejméně jeden roku, nebo trestu přísnějšímu.

   (b) Je-li třeba, v souladu s ujednáním dohodnutým na základě jednotných právních předpisů nebo reciproční právní úpravy, nebo se smlouvou o vydávání, včetně Evropské úmluvy o vydávání (ETS č. 24), použitelnými mezi dvěma nebo více stranami, použít jiný nejnižší trest, užije se nejnižší trest stanovený takovým ujednáním nebo smlouvou.

2. U trestných činů uvedených v odstavci 1 tohoto článku se má za to, že jsou zahrnuty jako trestné činy podléhající vydání do jakékoli úmluvy o vydávání existující mezi stranami. Strany se zavazují, že tyto trestné činy zahrnou mezi činy podléhající vydání do jakékoli úmluvy o vydávání, kterou mezi sebou uzavřou.

3. Pokud strana, jež podmiňuje vydání existencí smlouvy, obdrží žádost o vydání od jiné strany, se kterou neuzavřela smlouvu o vydávání, může tato strana považovat tuto Úmluvu za právní podklad pro vydání ve vztahu k jakémukoli trestnému činu uvedenému v odstavci 1 tohoto článku.

4. Strany, jež nepodmiňují vydání existencí smlouvy, budou uznávat trestné činy uvedené v odstavci 1 tohoto článku jako činy, pro které je mezi nimi vydání přípustné.

5. Na vydávání se budou vztahovat podmínky stanovené v právu dožádané strany nebo platné smlouvy o vydávání, včetně důvodů, pro které může dožádaná strana vydání odmítnout.

6. Pokud je vydání v případě trestného činu uvedeného v odstavci 1 tohoto článku odmítnuto výlučně z důvodu státní příslušnosti dotyčné osoby nebo z toho důvodu, že dožádaná

strana má za to, že se na trestný čin vztahuje její pravomoc, dožádaná strana předá na žádost dožadující strany věc svým příslušným orgánům pro účely trestního stíhání a v patřičnou dobu sdělí konečný výsledek dožadující straně. Tyto orgány učiní rozhodnutí a budou vést svá vyšetřování i řízení stejným způsobem jako v případě jakéhokoli jiného trestného činu srovnatelné povahy podle práva této strany.

7. (a) Každá strana sdělí při podpisu této Úmluvy, při uložení své ratifikační listiny, listiny o přijetí, schválení nebo přistoupení, generálnímu tajemníkovi Rady Evropy název a adresu každého orgánu odpovědného za předkládání nebo přijímání žádostí o vydání nebo o předběžnou vazbu v případě absence úmluvy.

(b) Generální tajemník Rady Evropy vytvoří a povede aktuální seznam orgánů takto určených stranami. Každá strana zajistí, aby údaje vedené v seznamu byly vždy správné.

Oddíl 3 – Obecné zásady týkající se vzájemné pomoci

Článek 25 – Obecné zásady týkající se vzájemné pomoci

1. Strany poskytnou jedna druhé vzájemnou pomoc v co možná nejširším rozsahu pro účely vyšetřování nebo řízení o trestných činech týkajících se počítačových systémů nebo dat, nebo pro účely shromažďování důkazů o trestném činu, které jsou v elektronické formě.

2. Každá strana také rovněž přijme taková legislativní nebo jiná opatření, která budou nezbytná k tomu, aby splnila závazky stanovené ve článcích 27 - 35.

3. Každá strana může, v naléhavých případech, podávat žádosti o vzájemnou pomoc nebo sdělení s ní spojená rychlými komunikačními prostředky, včetně faxu nebo elektronické pošty, do rozsahu v jakém takové prostředky poskytují přiměřenou úroveň bezpečnosti a ověření (včetně použití šifrování, je-li to nezbytné), a na žádost dožádané strany je následně formálně potvrdí. Dožádaná strana přijme a odpoví na dožádání jakýmkoli z těchto rychlých komunikačních prostředků.

4. Pokud není v článcích této kapitoly stanoveno jinak, bude se vzájemná pomoc řídit podmínkami stanovenými v právu dožádané strany nebo v příslušných úmluvách o vzájemné pomoci, včetně důvodů, pro které může dožádaná strana odmítnout spolupráci. Dožádaná strana neuplatní právo odmítnout pomoc ve vztahu k trestným činům uvedeným v článcích 2 – 11 výlučně proto, že se žádost vztahuje na trestný čin, který považuje za trestný čin fiskální.

5. V případech, kdy podle ustanovení této kapitoly může dožádaná strana poskytnutí vzájemné pomoci podmiňovat existencí dvojí trestnosti, bude se tato podmínka považovat za splněnou, pokud jednání tvořící trestný čin, ve vztahu k němuž se vyžaduje pomoc, je trestným činem podle jejího práva, bez ohledu na to, zda právo této strany klade tento trestný čin do stejné kategorie trestných činů nebo označuje tento trestný čin stejnou terminologií jako strana dožadující.

Článek 26 – Spontánní informace

1. Strana může v mezích svého vnitrostátního práva bez předchozí žádosti předat jiné straně informace získané v rámci svého vlastního vyšetřování, pokud má za to, že sdělení takových informací by mohlo pomoci přijímající straně při zahájení nebo provádění vyšetřování nebo řízení týkajících se trestných činů stanovených v souladu s touto Úmluvou, nebo že by mohlo vést k žádosti o spolupráci předloženou touto stranou v souladu s touto kapitolou.

2. Před poskytnutím takových informací může poskytující strana požadovat, aby byly utajeny nebo použity pouze za určitých podmínek. Pokud přijímající strana nemůže tento požadavek splnit, uvědomí poskytující stranu, která se pak rozhodne, zda přesto tyto informace poskytne. Pokud přijímající strana přijme informace za stanovených podmínek, bude jimi vázána.

Oddíl 4 - Postupy vztahující se na žádosti o vzájemnou pomoc při neexistenci příslušných mezinárodních dohod

Článek 27 - Postupy vztahující se na žádosti o vzájemnou pomoc při neexistenci příslušných mezinárodních dohod

1. V případech, kdy neexistuje mezi dožadující a dožádanou stranou smlouva o vzájemné pomoci nebo ujednání na základě jednotných právních předpisů nebo reciproční právní úpravy, použijí se ustanovení odstavců 2 až 9 tohoto článku. Ustanovení tohoto článku se nepoužijí, existují-li taková smlouva, ujednání nebo právní předpisy, pokud se zúčastněné strany nedohodnou, že budou místo nich uplatňovat všechna nebo některá zbývající ustanovení tohoto článku.

2. (a) Každá strana určí ústřední orgán nebo orgány, které budou zodpovědné za předkládání žádostí a odpovídání na žádosti o vzájemnou pomoc, vyřizování takových žádostí nebo jejich předávání orgánům příslušným pro jejich vyřizování.

(b) Ústřední orgány se budou stýkat přímo.

(c) Každá strana při podpisu této Úmluvy nebo při uložení své ratifikační listiny, listiny o přijetí, schválení nebo přistoupení k této Úmluvě, sdělí generálnímu tajemníkovi Rady Evropy názvy a adresy orgánů ustanovených podle tohoto odstavce.

(d) Generální tajemník Rady Evropy vytvoří a povede aktuální seznam ústředních orgánů takto stranami ustanovených. Každá strana zajistí, aby údaje vedené v seznamu byly vždy správné.

3. Žádosti o vzájemnou pomoc podle tohoto článku budou prováděny podle postupů určených dožadující stranou s výjimkou případů, kdy jsou neslučitelné s právem dožádané strany.

4. Dožádaná strana může, kromě důvodů pro odmítnutí stanovených v článku 25 odstavci (4), odmítnout pomoc, pokud:

   (a) se žádost týká trestného činu, který dožádaná strana považuje za politický trestný čin nebo za trestný čin spojený s politickým trestným činem; nebo

   (b) je názoru, že vyřízení žádosti by bylo zřejmě na újmu její svrchovanosti, bezpečnosti, veřejného pořádku nebo jiného základního zájmu.

5. Dožádaná strana může odložit provedení žádosti, pokud by to bylo na újmu trestnímu vyšetřování nebo řízení prováděnému jejími orgány.

6. Před odmítnutím nebo odložením pomoci zváží dožádaná strana, po případných konzultacích s dožadující stranou, zda je možno žádost provést částečně nebo za podmínek, které považuje za nezbytné.

7. Dožádaná strana bude bez prodlení informovat dožadující stranu o výsledku provedení žádosti o pomoc. Pokud bude žádost odmítnuta nebo odložena, je nutno uvést důvody jejího odmítnutí nebo odložení. Dožádaná strana bude také informovat dožadující stranu o jakýchkoli důvodech, které znemožňují provedení žádosti nebo je zřejmě významně zpozdí.

8. Dožadující strana může žádat, aby dožádaná strana uchovala v tajnosti podání žádosti podle této kapitoly, jakož i její obsah, kromě toho, co je nezbytné pro provedení žádosti. Pokud dožádaná strana nemůže splnit požadavek na utajení, urychleně o tom uvědomí dožadující stranu, která následně rozhodne, zda má být žádost přesto provedena.

9. (a) V případě naléhavosti je možno žádosti o vzájemnou pomoc nebo s nimi spojená sdělení zasílat přímo justičními orgány dožadující strany obdobným orgánům dožádané strany. V takových případech bude kopie zároveň zaslána ústřednímu orgánu dožádané strany prostřednictvím ústředního orgánu dožadující strany.

   (b) Jakoukoli žádost nebo sdělení podle tohoto odstavce lze učinit prostřednictvím Mezinárodní organizace kriminální policie (Interpol).

   (c) Pokud je učiněna žádost podle pododstavce (a) orgánu nepříslušnému k vyřízení žádosti, předá tento orgán žádost k provedení příslušnému státnímu orgánu a informuje o tom dožadující stranu.

   (d) Žádosti nebo sdělení učiněná podle tohoto odstavce, která nepředpokládají použití donucovacích opatření, mohou příslušné orgány dožadující strany předat přímo příslušným orgánům dožádané strany.

   (e) Každá strana může při podpisu této Úmluvy, při uložení své ratifikační listiny nebo listiny o přijetí, schválení nebo přistoupení k této Úmluvě, sdělit generálnímu tajemníkovi Rady Evropy, že z důvodů efektivity mají být žádosti podle tohoto odstavce adresovány jejímu ústřednímu orgánu.

Článek 28 – Utajení a omezení použití

1. Pokud není mezi dožadující a dožádanou stranou v platnosti smlouva o vzájemné pomoci nebo ujednání na základě jednotných právních předpisů nebo reciproční právní úpravy, použijí se ustanovení tohoto článku. Existuje-li taková smlouva, ujednání nebo právní předpisy, ustanovení tohoto článku se nepoužijí, vyjma těch případů, kdy se zúčastněné strany namísto toho dohodnou na použití některého nebo všech zbývajících ustanovení tohoto článku.

2. Dožádaná strana může poskytnutí informací nebo podkladů při odpovědi na žádost podmínit tím, že tyto informace a podklady:

   a) budou utajeny, pokud by žádosti o vzájemnou právní pomoc nebylo možno vyhovět bez takové podmínky, nebo

   b) nebudou použity pro jiná vyšetřování nebo řízení než pro ta, která jsou uvedena v žádosti.

3. Pokud dožadující strana nemůže vyhovět podmínkám uvedeným v odstavci 2, urychleně uvědomí druhou stranu, která poté rozhodne, zda bude informace přesto poskytnuta. Pokud dožadující strana přijme podmínku, bude jí vázána.

4. Každá strana, která poskytne informace nebo podklady za podmínky uvedené v odstavci 2 může požadovat od druhé strany, aby jí informovala o tom, jak v souvislosti s touto podmínkou použila takové informace nebo podklady.

Část 2 – Zvláštní ustanovení

Oddíl 1 – Vzájemná právní pomoc týkající se prozatímních opatření

Článek 29 – Urychlené uchování uložených počítačových dat

1. Strana může požádat jinou stranu, aby nařídila nebo jinak zajistila urychlené uchování dat uložených prostřednictvím počítačového systému, který je umístěn na území této druhé strany, a která mají být předmětem žádosti dožadující strany o vzájemnou pomoc týkající se prohlídky nebo získání přístupu obdobným způsobem, zajištění nebo obdobného zabezpečení, či zpřístupnění těchto dat.

2. V žádosti o uchování předložené podle odstavce 1 se uvede:

   (a) orgán, který o uchování žádá;

   (b) trestný čin, který je předmětem vyšetřování nebo řízení a stručné shrnutí souvisejících skutečností;

   (c) uložená počítačová data, která mají být uchována a jejich souvislost s trestným činem;

(d) jakákoli dostupná informace pro zjištění správce uložených počítačových dat nebo umístění počítačového systému;

(e) důvod nezbytnosti uchovat data; a

(f) záměr strany předložit žádost o vzájemnou pomoc týkající se prohlídky nebo získání přístupu obdobným způsobem, zajištění nebo obdobného zabezpečení nebo zpřístupnění dat.

3. Po obdržení žádosti od jiné strany podnikne dožádaná strana veškerá příslušná opatření, aby urychleně uchovala specifikovaná data, v souladu se svými vnitrostátními právními předpisy. Pro účely vyřízení žádosti nebude oboustranná trestnost vyžadována jako podmínka provedení takového uchování.

4. Strana, která požaduje oboustrannou trestnost jako podmínku pro vyřízení žádosti o vzájemnou pomoc týkající se prohlídky nebo podobného přístupu, zajištění nebo podobného zabezpečení, nebo zpřístupnění dat, si může, ve vztahu k trestným činům jiným než jsou ty stanovené v souladu s články 2 – 11 této Úmluvy, vyhradit právo odmítnout žádost o uchování podle tohoto článku v případech, kdy má důvod předpokládat, že v době zpřístupnění by nebylo možno podmínku dvojí trestnosti naplnit.

5. Dále může být žádost o uchování odmítnuta pouze pokud:

(a) se žádost týká trestného činu, který dožádaná strana považuje za politický čin nebo trestný čin spojený s politickým trestným činem; nebo

(b) je dožádaná strana toho názoru, že provedení žádosti by bylo zřejmě na újmu její svrchovanosti, bezpečnosti, veřejnému pořádku nebo jiným základním zájmům.

6. V případech, kdy se dožádaná strana domnívá, že pouhé uchování nezajistí budoucí dostupnost dat nebo ohrozí utajení či jiným způsobem naruší vyšetřování dožadující strany, bez prodlení to sdělí dožadující straně, která pak rozhodne, zda má být žádost přesto vyřízena.

7. Žádné uchování provedené na základě žádosti uvedené v odstavci 1 nebude trvat méně než 60 dní, aby dožadující strana mohla předložit žádost o prohlídku nebo podobný přístup, zajištění nebo podobné zabezpečení či zpřístupnění dat. Po obdržení takové žádosti budou data i nadále uchována, až do rozhodnutí o této žádosti.

Článek 30 – Urychlené sdělení uchovaných provozních dat

1. Pokud během provádění žádosti předložené podle článku 29 o uchování provozních dat týkajících se určité komunikace dožádaná strana zjistí, že poskytovatel služeb v jiném státě byl zapojen do přenosu této komunikace, dožádaná strana urychleně sdělí dožadující straně dostatečné množství provozních dat, aby bylo možno identifikovat tohoto poskytovatele služeb a cestu, jíž byla komunikace přenesena.

2. Sdělení provozních dat podle odstavce 1 může být odmítnuto pouze pokud:

(a) se žádost týká trestného činu, který dožádaná strana považuje za politický trestný čin nebo za trestný čin spojený s politickým trestným činem;

(b) je dožádaná strana toho názoru, že provedení žádosti by bylo zřejmě na újmu její svrchovanosti, bezpečnosti, veřejnému pořádku nebo jiným základním zájmům.

Oddíl 2 – Vzájemná pomoc týkající se vyšetřovacích pravomocí

Článek 31 – Vzájemná pomoc týkající se přístupu k uloženým počítačovým datům

1. Strana může požádat jinou stranu, aby ohledně dat, uložených prostřednictvím počítačového systému umístěného na území dožádané strany, včetně dat uchovaných podle článku 29, provedla prohlídku nebo k nim podobným způsobem získala přístup, zabavila je nebo je podobným způsobem zajistila a zpřístupnila.

2. Při vyřizování žádosti použije dožádaná strana mezinárodní dokumenty, ujednání a právní předpisy uvedené v článku 23 jakož i další příslušná ustanovení této kapitoly.

3. Žádost se vyřídí urychleně, pokud:

(a) lze předpokládat, že příslušná data jsou zvláště ohrožená ztrátou nebo pozměněním; nebo

(b) je rychlá spolupráce jinak stanovena dokumenty, ujednáními a právními předpisy uvedenými v odstavci 2.

Článek 32 – Přeshraniční přístup k uloženým počítačovým datům veřejně dostupným nebo se souhlasem

Strana může bez získání povolení jiné strany:

(a) získat přístup k veřejně dostupným uloženým počítačovým datům (z otevřeného zdroje) bez ohledu na to, kde jsou data geograficky umístěna; nebo

(b) pomocí počítačového systému na svém území buď získat přístup k uloženým počítačovým datům umístěným na území jiné strany, nebo tato data obdržet, pokud tato strana získá právoplatný a dobrovolný souhlas osoby, která má zákonnou pravomoc zpřístupnit straně data pomocí tohoto počítačového systému.

Článek 33 – Vzájemná pomoc týkající se shromažďování provozních dat v reálném čase

1. Strany si budou poskytovat vzájemnou pomoc při shromažďování provozních dat v reálném čase souvisejících s určenými komunikacemi na svém území, přenášenými pomocí počítačového systému. V souladu s odstavcem 2 se na tuto pomoc budou vztahovat podmínky a postupy stanovené vnitrostátním právním řádem.

2. Každá strana poskytne tuto pomoc alespoň ve vztahu k trestným činům, u nichž by bylo shromažďování dat v reálném čase přípustné v podobných vnitrostátních případech.

Článek 34 – Vzájemná pomoc týkající se odposlechu obsahových dat

Strany si budou poskytovat vzájemnou pomoc při shromažďování nebo zaznamenávání, a to v reálném čase, obsahových dat určených komunikací, přenášených pomocí počítačového systému v rozsahu, ve kterém to umožňují příslušné smlouvy a vnitrostátní právní předpisy.

Oddíl 3 – Síť 24/7

Článek 35 - 24/7 Síť

1. Každá strana určí kontaktní místo, jež bude k dispozici 24 hodin denně, 7 dnů v týdnu, aby bylo možné poskytovat okamžitou pomoc pro účely vyšetřování nebo řízení ohledně trestných činů spojených s počítačovými systémy a daty, nebo pro shromažďování důkazů v elektronické formě o trestném činu. Tato pomoc bude zahrnovat usnadňování nebo, pokud to dovolují vnitrostátní právní předpisy a praxe této strany, i přímé provádění následujících opatření:

   (a) poskytování technických rad;

   (b) uchování dat podle článků 29 a 30; a

   (c) shromažďování důkazů, poskytování právních informací a lokalizování podezřelých osob.

2. (a) Kontaktní místo strany bude způsobilé ke zrychlené komunikaci s kontaktním místem jiné strany.

   (b) Pokud kontaktní místo určené stranou není součástí orgánu nebo orgánů této strany příslušných pro mezinárodní vzájemnou pomoc nebo vydávání, zajistí toto kontaktní místo, že je schopno urychlené koordinace s takovým orgánem nebo orgány.

3. Každá strana zajistí za účelem usnadnění provozu sítě zaškolený a vybavený personál.

Kapitola IV – Závěrečná ustanovení

Článek 36 – Podpis a vstup v platnost

1. Tato Úmluva bude otevřena k podpisu členským státům Rady Evropy a nečlenským státům, které se účastnily jejího vypracování.

2. Tato Úmluva podléhá ratifikaci, přijetí nebo schválení. Ratifikační listiny, listiny o přijetí nebo schválení budou uloženy u generálního tajemníka Rady Evropy.

3. Tato Úmluva vstoupí v platnost první den měsíce následujícího po uplynutí období tří měsíců po dni, kdy pět států, včetně nejméně tří členských států Rady Evropy, vyjádřilo

svůj souhlas s tím, že pro ně bude Úmluvou závazná, v souladu s ustanoveními odstavců 1 a 2.

4. Pro kterýkoli signatářský stát, který následně vyjádří svůj souhlas s tím, že pro něj bude Úmluva závazná, vstoupí Úmluva v platnost první den měsíce následujícího po uplynutí období tří měsíců po dni, kdy vyjádřil svůj souhlas s tím, že pro něj bude Úmluva závazná podle ustanovení odstavců 1 a 2.

Článek 37 – Přístup k Úmluvě

1. Po vstupu této Úmluvy v platnost může Výbor ministrů Rady Evropy, po konzultaci se smluvními státy Úmluvy a po obdržení jejich jednomyslného souhlasu, přizvat kterýkoli stát, který není členem Rady a neúčastnil se jejího vypracování, aby přistoupil k této Úmluvě. Rozhodnutí bude přijato většinou stanovenou článkem 20 (d) Statutu Rady Evropy a jednomyslným hlasováním zástupců smluvních států oprávněných zasedat ve Výboru ministrů.

2. Pro kterýkoli stát přistupující k Úmluvě podle odstavce 1 shora vstoupí Úmluva v platnost první den měsíce následujícího po uplynutí tří měsíců po dni uložení listiny o přístupu u generálního tajemníka Rady Evropy.

Článek 38 – Územní působnost

1. Každý stát může při podpisu této Úmluvy nebo při uložení své ratifikační listiny, listiny o přijetí, schválení nebo přístupu určit jedno nebo více území, na kterých se bude provádět tato Úmluva.

2. Každá strana může následně, formou prohlášení zaslaného generálnímu tajemníkovi Rady Evropy, rozšířit působnost této Úmluvy na jakékoli jiné území uvedené v prohlášení. Pro takové území vstoupí Úmluva v platnost první den měsíce následujícího po uplynutí tří měsíců po dni, kdy generální tajemník obdrží toto prohlášení.

3. Jakékoli prohlášení podle dvou výše uvedených odstavců může být, ohledně jakéhokoli území uvedeného v takovém prohlášení, odvoláno oznámením adresovaným generálnímu tajemníkovi Rady Evropy. Odvolání nabude účinnosti první den měsíce následujícího po uplynutí období tří měsíců po dni, kdy generální tajemník obdrží takové oznámení.

Článek 39 – Účinky Úmluvy

1. Účelem této Úmluvy je doplnit příslušné multilaterální nebo bilaterální smlouvy nebo ujednání mezi stranami, včetně ustanovení:

   - Evropské úmluvy o vydávání otevřené k podpisu ve Štrasburku 13. prosince 1957 (ETS č. 24);

   - Evropské úmluvy o vzájemné pomoci ve věcech trestních otevřené k podpisu ve Štrasburku 20. dubna 1959 (ETS č. 30);

- Dodatkového protokolu k Evropské úmluvě o vzájemné pomoci ve věcech trestních otevřeného k podpisu ve Štrasburku 17. března 1978 (ETS č. 99).

2. Pokud dvě nebo více stran již uzavřelo smlouvu nebo dohodu ve věcech, jež jsou předmětem této Úmluvy, nebo jinak upravily své vztahy v těchto věcech, nebo pokud by tak v budoucnu učinily, budou rovněž oprávněny příslušně uplatňovat takovou smlouvu nebo dohodu nebo upravit tyto vzájemné vztahy. Pokud však strany upraví své vztahy ve věcech, jež jsou předmětem této Úmluvy, jinak, než Úmluva stanoví, učiní tak způsobem, který neodporuje cílům a principům Úmluvy.

3. Nic v této Úmluvě se nedotýká jiných práv, omezení, závazků a povinností stran.

Článek 40 – Prohlášení

Písemným oznámením adresovaným generálnímu tajemníkovi Rady Evropy může kterýkoli stát při podpisu nebo při uložení své ratifikační listiny, listiny o přijetí, schválení nebo přístupu prohlásit, že využívá možnosti požadovat dodatečné prvky stanovené podle článku 2, článku 3, článku 6, odstavce 1 písm. b), článku 7, článku 9, odstavce 3 a článku 27, odstavce 9 písm. e).

Článek 41 – Federální doložka

1. Federální stát si může vyhradit právo převzít závazky podle Kapitoly II této Úmluvy v souladu s jeho základními principy upravujícími vztah mezi jeho ústřední vládou a jednotlivými státy spolku nebo jinými podobnými územními jednotkami, za předpokladu, že je stále způsobilý spolupracovat podle Kapitoly III.

2. Při uplatnění výhrady podle odstavce 1 nesmí federální stát použít podmínky takové výhrady tak, aby vyloučil nebo podstatně umenšil své závazky přijmout opatření uvedená v Kapitole II. Zásadně poskytne širokou a účinnou schopnost vynucování zákona s ohledem na tato opatření.

3. S ohledem na ta ustanovení Úmluvy, jejichž provedení spadá do pravomoci jednotlivých států federace nebo jiných podobných územních jednotek, které nejsou podle ústavního systému federálního státu povinny přijmout zákonodárná opatření, bude spolková vláda informovat příslušné orgány těchto států o uvedených ustanoveních se svým příznivým názorem, vybízejíc je k přijetí příslušných kroků k jejich provedení.

Článek 42 – Výhrady

Písemným oznámením zaslaným generálnímu tajemníkovi Rady Evropy může každý stát při podpisu nebo při uložení své ratifikační listiny, listiny o přijetí, schválení nebo přístupu prohlásit, že využívá výhrad podle článku 4, odstavce 2, článku 6, odstavce 3, článku 9, odstavce 4, článku 10, odstavce 3, článku 11, odstavce 3, článku 14, odstavce 3, článku 22, odstavce 2, článku 29, odstavce 4 a článku 41, odstavce 1. Jinou výhradu nelze učinit.

Článek 43 – Stav a odvolání výhrad

1. Strana, která učinila výhradu podle článku 42, ji může zcela nebo částečně odvolat oznámením zaslaným generálnímu tajemníkovi Rady Evropy. Toto odvolání nabude účinnosti v den, kdy je obdrží generální tajemník. Pokud je v oznámení uvedeno, že odvolání výhrady má nabýt účinnosti k datu uvedenému v tomto oznámení a toto datum je pozdější než datum, kdy generální tajemník obdržel toto oznámení, odvolání nabude účinnosti k tomuto pozdějšímu datu.

2. Strana, která učinila výhradu podle článku 42 tuto výhradu zcela nebo částečně odvolá, jakmile to okolnosti dovolí.

3. Generální tajemník se může pravidelně dotazovat stran, které učinily jednu nebo více výhrad podle článku 38, jaké jsou vyhlídky na odvolání výhrad(y).

Článek 44 - Dodatky

1. Dodatky k této Úmluvě může navrhnout kterákoli strana, a generální tajemník Rady Evropy je sdělí členským státům Rady Evropy, nečlenským státům, které se účastnily vypracování této Úmluvy i kterémukoli jinému státu, který přistoupil nebo byl přizván k přístupu k této Úmluvě v souladu s ustanovením článku 37.

2. Každý dodatek navržený stranou bude sdělen Evropskému výboru pro problémy kriminality (CDPC), který Výboru ministrů předloží svůj názor na navrhovaný dodatek.

3. Výbor ministrů zváží navrhovaný dodatek a názor předložený Evropským výborem pro problémy kriminality (CDPC) a, po konzultacích s nečlenskými státy, jež jsou stranami této Úmluvy, může dodatek schválit.

4. Text každého dodatku schváleného Výborem ministrů v souladu s odstavcem 3 tohoto článku bude předložen stranám k přijetí.

5. Každý dodatek přijatý podle odstavce 3 tohoto článku vstoupí v platnost třicátý den poté, co všechny strany informovaly generálního tajemníka o tom, že dodatek přijímají.

Článek 45 – Urovnání sporů

1. Evropský výbor Rady Evropy pro problémy kriminality (CDPC) bude informován o výkladu a provádění této Úmluvy.

2. V případě sporu mezi stranami ohledně výkladu nebo provádění této Úmluvy se strany budou snažit o řešení sporu jednáním nebo jinými smírnými prostředky dle své vlastní volby, včetně předložení sporu Evropskému výboru pro problémy kriminality nebo rozhodčímu soudu, jehož rozhodnutí budou pro strany závazná, nebo Mezinárodnímu soudnímu dvoru, a to podle dohody dotyčných stran.

Článek 46 – Porady stran

1. Strany se budou podle potřeby pravidelně radit za účelem usnadnění:

(a) účinného používání a provádění této Úmluvy, včetně identifikace všech problémů s tím spojených, i účinků jakéhokoli prohlášení nebo výhrad učiněných podle této Úmluvy;

(b) výměny informací o významných obecných, právních nebo technologických změnách týkajících se počítačové kriminality a shromažďování důkazů v elektronické formě;

(c) zvážení možného doplnění nebo změny Úmluvy.

2. Evropský výbor pro problémy kriminality (CDPC) bude pravidelně informován o výsledku konzultací uvedených v odstavci 1.

3. Evropský výbor pro problémy kriminality (CDPC) bude podle potřeby usnadňovat porady uvedené v odstavci 1 a přijímat opatření nezbytná k tomu, aby pomohl stranám v jejich úsilí o doplnění nebo změnu Úmluvy. Nejpozději tři roky po vstupu této Úmluvy v platnost provede Evropský výbor pro problémy kriminality (CDPC) ve spolupráci se stranami revizi všech ustanovení Úmluvy a doporučí jakékoli vhodné změny, bude-li to nezbytné.

4. Náklady vzniklé při provádění ustanovení odstavce 1 budou hrazeny stranami způsobem, který samy určí, s výjimkou nákladů převzatých Radou Evropy.

5. Sekretariát Rady Evropy bude stranám ku pomoci při provádění činností podle tohoto článku.

Článek 47 - Výpověď

1. Každá strana může kdykoliv vypovědět tuto Úmluvu oznámením adresovaným generálnímu tajemníkovi Rady Evropy.

2. Taková výpověď nabude účinnosti první den měsíce následujícího po uplynutí tří měsíců od obdržení oznámení generálním tajemníkem.

Článek 48 – Oznámení

Generální tajemník Rady Evropy bude informovat členské státy Rady Evropy, nečlenské státy, jež se účastnily vypracování této Úmluvy i kterýkoli jiný stát, který přistoupil nebo byl přizván k přístupu k této Úmluvě, o:

(a) všech podpisech;

(b) uložení všech ratifikačních listin nebo listin o přijetí, schválení nebo přístupu;
(c) datu vstupu této Úmluvy v platnost v souladu s články 36 a 37;

(d) všech prohlášeních učiněných podle článku 40 nebo o všech výhradách učiněných v souladu s článkem 42;

(e) jakémkoli jiném úkonu, oznámení nebo sdělení vztahujícímu se k této Úmluvě.

Na důkaz výše uvedeného níže podepsaní, jsouce k tomu řádně zmocněni, podepsali tuto Úmluvu.

Dáno v Budapešti, dne 23. listopadu 2001, v jazyce anglickém a francouzském jazyce, přičemž obě znění mají stejnou platnost, v jednom vyhotovení, které bude uloženo v archivu Rady Evropy. Generální tajemník Rady Evropy předá ověřené opisy každému členskému státu Rady Evropy, nečlenským státům, jež se účastnily vypracování této Úmluvy a kterémukoli jinému státu přizvanému k přístupu k této Úmluvě.

ISSN 1801-0393

Vydává a tiskne: Tiskárna Ministerstva vnitra, p. o., Bartůňkova 4, pošt. schr. 10, 149 01 Praha 415, telefon: 272 927 011, fax: 974 887 395 – **Redakce**: Ministerstvo vnitra, nám. Hrdinů 1634/3, pošt. schr. 155/SB, 140 21 Praha 4, telefon: 974 817 289, fax: 974 816 871 – **Administrace**: písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – MORAVIAPRESS, a. s., U Póny 3061, 690 02 Břeclav, tel.: 516 205 175, e-mail: sbirky@moraviapress.cz. Objednávky ve Slovenské republice přijímá a titul distribuuje Magnet-Press Slovakia, s. r. o., Teslova 12, 821 02 Bratislava, tel.: 00421 2 44 45 46 28, fax: 00421 2 44 45 46 27. **Roční předplatné** se stanovuje za dodávku kompletního ročníku včetně rejstříku z předcházejícího roku a je od předplatitelů vybíráno formou záloh ve výši oznámené ve Sbírce mezinárodních smluv. Závěrečné vyúčtování se provádí po dodání kompletního ročníku na základě počtu skutečně vydaných částek (první záloha na rok 2013 činí 6 000,– Kč, druhá záloha na rok 2013 činí 6 000,– Kč, třetí záloha na rok 2013 činí 4 000,– Kč) – Vychází podle potřeby – **Distribuce**: MORAVIAPRESS, a. s., U Póny 3061, 690 02 Břeclav, celoroční předplatné a objednávky jednotlivých částek (dobírky) – 516 205 175, objednávky-knihkupci – 516 205 175, e-mail – sbirky@moraviapress.cz, zelená linka – 800 100 314. **Internetová prodejna**: www.sbirkyzakonu.cz – **Drobný prodej – Brno**: Ing. Jiří Hrazdil, Vranovská 16, SEVT, a. s., Česká 14; **České Budějovice**: SEVT, a. s., Česká 3, tel.: 387 319 045; **Cheb**: EFREX, s. r. o., Karlova 31; **Chomutov**: DDD Knihkupectví – Antikvariát, Ruská 85; **Kadaň**: Knihařství – Přibíková, J. Švermy 14; **Liberec**: Podještědské knihkupectví, Moskevská 28; **Olomouc**: Zdeněk Chumchal – Knihkupectví Tycho, Ostružnická 3; **Ostrava**: LIBREX, Nádražní 14; **Otrokovice**: Ing. Kučeřík, Jungmannova 1165; **Pardubice**: ABONO s. r. o., Sportovců 1121, LEJHANEC, s. r. o., třída Míru 65; **Plzeň**: Vydavatelství a nakladatelství Aleš Čeněk, nám. Českých bratří 8; **Praha 3**: Vydavatelství a nakladatelství Aleš Čeněk, K Červenému dvoru 24; **Praha 4**: Tiskárna Ministerstva vnitra, Bartůňkova 4; **Praha 6**: PERIODIKA, Komornická 6; **Praha 9**: Abonentní tiskový servis-Ing. Urban, Jablonecká 362, po – pá 7 – 12 hod., tel.: 286 888 382, e-mail: tiskovy.servis@top-dodavatel.cz, DOVOZ TISKU SUWECO CZ, Klečákova 347; **Praha 10**: BMSS START, s. r. o., Vinohradská 190, MONITOR CZ, s. r. o., Třebohostická 5, tel.: 283 872 605; **Přerov**: Jana Honková-YAHO-i-centrum, Komenského 38; **Ústí nad Labem**: PNS Grosso s. r. o., Havířská 327, tel.: 475 259 032, fax: 475 259 029; **Zábřeh**: Mgr. Ivana Patková, Žižkova 45; **Žatec**: Jindřich Procházka, Bezděkov 89 – Vazby Sbírek, tel.: 415 712 904. **Distribuční podmínky předplatného**: jednotlivé částky jsou expedovány neprodleně po dodání z tiskárny. Objednávky nového předplatného jsou vyřizovány do 15 dnů a pravidelné dodávky jsou zahajovány od nejbližší částky po ověření úhrady předplatného nebo jeho zálohy. Částky vyšlé v době od zaevidování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. **Reklamace**: informace na tel. čísle 516 205 175. V písemném styku vždy uvádějte IČO (právnická osoba), rodné číslo (fyzická osoba). **Podávání novinových zásilek** povoleno Českou poštou, s. p., Odštěpný závod Jižní Morava Ředitelství v Brně č. j. P/2-4463/95 ze dne 8. 11. 1995.