HRVATSKI SABOR

Na temelju članka 88. Ustava Republike Hrvatske, donosim

ODLUKU

O PROGLAŠENJU ZAKONA O POTVRĐIVANJU KONVENCIJE O KIBERNETIČKOM KRIMINALU

Proglašavam Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu, koji je donio Hrvatski sabor na sjednici 3. srpnja 2002.

Broj: 01-081-02-2622/2
Zagreb, 8. srpnja 2002.

Predsjednik
Republike Hrvatske
Stjepan Mesić, v. r.

ZAKON

O POTVRĐIVANJU KONVENCIJE O KIBERNETIČKOM KRIMINALU

Članak 1.

Potvrđuje se Konvencija o kibernetičkom kriminalu, usvojena na konferenciji Vijeća Europe u Budimpešti, a koju je Republika Hrvatska potpisala 23. studenoga 2001.

Članak 2.

Tekst Konvencije o kibernetičkom kriminalu, u izvorniku na engleskom jeziku i u prijevodu na hrvatski jezik, glasi:

CONVENTION ON CYBERCRIME

PREAMBLE

The member States of the Council of Europe and the other States signatory hereto,
Considering that the aim of the Council of Europe is to achieve a greater unity between its members;
Recognising the value of fostering co-operation with the other States parties to this Convention;
Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;
Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;
Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;
Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;
Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;
Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;
Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;
Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;
Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;
Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;
Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R. (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the

use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

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

Have agreed as follows.

Chapter I – USE OF TERMS

Article 1 – DEFINITIONS

For the purposes of this Convention:

a *»computer system«* means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b *»computer data«* means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c *»service provider«* means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d *»traffic data«* means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communicationžs 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 supressing 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 possesion referred to in paragraph 1 of this article is not for the purpose of committing an offences 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 1 – 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 l 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, subparagraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – OFFENCES RELATED TO INFRINGEMENTS OF COPYRIGHT AND RELATED RIGHTS

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International

Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Partyžs 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 noncriminal sanctions or measures,

including monetary sanctions.

Section 2 – PROCEDURAL LAW

Title 1 – Common provisions

Article 14 – SCOPE OF PROCEDURAL PROVISIONS

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system, and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – CONDITIONS AND SAFEGUARDS

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – EXPEDITED PRESERVATION OF STORED COMPUTER DATA

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the personžs 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 pocedures 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 Partyžs 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 personžs 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 provideržs 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 subscriberžs 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 of 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 i or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – REAL-TIME COLLECTION OF TRAFFIC DATA

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means

on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – INTERCEPTION OF CONTENT DATA

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – JURISDICTION

Article 22 – JURISDICTION

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party, or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – INTERNATIONAL CO-OPERATION

Section 1 – GENERAL PRINCIPLES

Title 1 – General principles relating to international co-operation

Article 23 – GENERAL PRINCIPLES RELATING TO INTERNATIONAL CO-OPERATION

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – EXTRADITION

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the condition 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 Article 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 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 right 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 on 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;

c 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 Partyžs 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, te requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – MUTUAL ASSISTANCE REGARDING ACCESSING OF STORED COMPUTER DATA

1 A Party may request another Party to search or similarly access, seize or similarly secure,

and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are ground 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 Partyžs 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 Partyžs authority or authorities responsible for international mutual assistance of 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, te 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 aplication 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 entiled 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 Conventionžs objectives and principles.

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

Article 40 – DECLARATIONS

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – FEDERAL CLAUSE

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

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

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

Article 42 – RESERVATIONS

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4,

paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – STATUS AND WITHDRAWAL OF RESERVATIONS

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

KONVENCIJA O KIBERNETIČKOM KRIMINALU

PREAMBULA

Države članice Vijeća Europe i ostale države potpisnice ove Konvencije

smatrajući da je cilj Vijeća Europe postići veće zajedništvo između njegovih članica;

priznajući vrijednost njegovanja suradnje s ostalim državama strankama ove Konvencije;

uvjerene da je potreba vođenja zajedničke kaznene politike usmjerene s zaštiti društva od kibernetičkog kriminala od prvenstvene važnosti, i to među ostalim i putem usvajanja odgovarajućeg zakonodavstva i poticanjem međunarodne suradnje;

svjesne dubokih promjena nastalih digitalizacijom, konvergencijom i neprekidnom globalizacijom računalnih mreža;

zabrinute zbog mogućnosti da računalne mreže i elektroničke informacije budu iskorištene za počinjenje kaznenih djela, te da dokazi vezani uz ta djela budu pohranjeni i prenošeni putem tih mreža;

prepoznajući potrebu za suradnjom između država i privatnog gospodarstva u borbi protiv kibernetičkog kriminala i potrebu za zaštitom legitimnih interesa prilikom korištenja i razvitka informatičkih tehnologija;

vjerujući da učinkovita borba protiv kibernetičkog kriminala zahtijeva povećanu, brzu i uhodanu međunarodnu suradnju u kaznenopravnim predmetima;

uvjerene da je ova Konvencija nužna radi odvraćanja od postupaka usmjerenih protiv tajnosti, cjelovitosti i dostupnosti računalnih sustava, mreža i računalnih podataka, kao i za odvraćanje od njihovih zloporaba, jer utvrđuje – na način opisan u ovoj Konvenciji – kriminalizaciju takvog ponašanja, usvaja ovlaštenja dovoljna za učinkovitu borbu protiv takvih kaznenih djela, olakšavajući time otkrivanje, istraživanje i kazneni progon tih kaznenih djela, kako na domaćoj, tako i na međunarodnoj razini, te osiguravajući brzu i pouzdanu međunarodnu suradnju;

imajući na umu potrebu za osiguranjem odgovarajuće ravnoteže između interesa provedbe zakona i poštivanja temeljnih ljudskih prava utjelovljenih u Konvenciji Vijeća Europe o zaštiti prava i temeljnih sloboda čovjeka iz 1950. godine, u Međunarodnom paktu Ujedinjenih naroda o građanskim i političkim pravima iz 1966. godine, kao i u drugim relevantnim međunarodnim sporazumima o ljudskim pravima koji ponovno potvrđuju svačije pravo na vlastito mišljenje bez mješanja izvana, pravo na slobodu izražavanja, uključujući i slobodu traženja, primanja i davanja informacija i ideja svih vrsta, bez obzira na granice, kao i prava koja se tiču poštivanja privatnosti;

imajući također na umu zaštitu osobnih podataka propisanu npr. Konvencijom Vijeća Europe o zaštiti pojedinaca s obzirom na automatsku obradu osobnih podataka iz 1981. godine;

imajući u vidu Konvenciju Ujedinjenih naroda o pravima djeteta iz 1989. godine i Konvenciju Međunarodne organizacije rada o najgorim oblicima dječjeg rada iz 1999. godine;

vodeći računa o postojećim konvencijama Vijeća Europe o suradnji na polju izvršenja kazni i sličnim sporazumima koji su na snazi između država članica Vijeća Europe i drugih država, te naglašavajući da je namjera ove Konvencije dopuniti navedene konvencije kao bi se kriminalističke istrage i postupci povodom kaznenih djela povezanih s računalnim sustavima i podacima učinili učinkovitijima, te kako bi se omogućilo prikupljanje dokaza o kaznenim djelima u elektroničkom obliku;

pozdravljajući nedavni razvitak događaja koji dodatno unapređuje međunarodno razumijevanje i suradnju u borbi protiv kibernetičkog kriminala, uključujući i postupke Ujedinjenih naroda, OECD-a, Europske unije i zemalja G8;

pozivajući se na Preporuku br. R (85) 10 o praktičnoj provedbi Europske konvencije o uzajamnoj pomoći u kaznenim predmetima u pogledu pružanja međunarodne pravne pomoći pri presretanju telekomunikacija, Preporuku br. R (88) 2 o piratstvu na polju autorskih i srodnih prava, Preporuku br. R (87) 15 koja propisuje uporabu osobnih podataka u oblasti djelatnosti policije,

Preporuku br. R (95) 4 o zaštiti osobnih podataka na području telekomunikacijskih usluga s posebnim osvrtom na usluge telefonije, Preporuku br. R (89) 9 o računalnom kriminalu koja daje smjernice nacionalnim zakonodavnim tijelima u pogledu definiranja određenih računalnih kaznenih djela, te Preporuku br. R (95) 13 o problemima kaznenog postupovnog prava vezanima uz informatičku tehnologiju;

s obzirom na Rezoluciju br. 1 usvojenu po europskim ministrima pravosuđa na njihovoj 21. konferenciji održanoj u Pragu u srpnju 1997. godine, a kojom se Odboru ministara preporučuje da podupre rad Europskog odbora za probleme kriminaliteta (European Committee on Crime Problems – CDPC) vezan uz kibernetički kriminal, kako bi se unutarnje odredbe kaznenog prava približile jedne drugima i kako bi se omogućilo korištenje učinkovitih istražnih sredstava u pogledu tih kaznenih djela, te s obzirom na Rezoluciju br. 3 usvojenu na 23. konferenciji europskih ministara pravosuđa u Londonu u lipnju 2000. godine, koja je ohrabrila strane u pregovorima da nastave s naporima u cilju nalaženja odgovarajućih rješenja kako bi se najvećem mogućem broju država omogućilo da postanu strankama Konvencije, te koja je potvrdila potrebu za brzim i učinkovitim sustavom međunarodne suradnje svjesnim specifičnih zahtjeva borbe protiv kibernetičkog kriminala;

te s obzirom na Akcijski plan o traženju zajedničkih odgovora na razvitak novih informatičkih tehnologija zasnovanih na standardima i vrijednostima Vijeća Europe, kojega su usvojili šefovi država i vlada Vijeća Europe na Drugom summitu u Strasbourgu dne. 10. i 11. listopada 1997. godine;

Sporazumijevaju se kako slijedi:

Poglavlje I. – POJMOVI

Članak 1. – DEFINICIJE

U ovoj Konvenciji:

a. izraz »računalni sustav« označava svaku napravu ili skupinu međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovu programa automatski obrađuju podatke;

b. izraz »računalni podaci« označava svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u računalnom sustavu, uključujući i program koji je u stanju prouzročiti da računalni sustav izvrši određenu funkciju;

c. izraz »davatelj usluga« označava:

i. svaki javni ili privatni entitet koji korisnicima svojih usluga omogućava komuniciranje pomoću računalnog sustava i

ii. svaki drugi entitet koji obrađuje ili pohranjuje računalne podatke za takvu komunikacijsku službu ili korisnike te službe;

d. izraz »podaci o prometu« označava sve računalne podatke u vezi komunikacija, koji su stvoreni pomoću računalnog sustava koji je dio komunikacijskog lanca, a koji podaci naznačuju podrijetlo komunikacije, njeno odredište, put, vrijeme, datum, veličinu, trajanje ili vrstu te usluge.

Poglavlje II. – MJERE KOJE TREBA PODUZETI NA NACIONALNOJ RAZINI

Odjeljak 1. – KAZNENO MATERIJALNO PRAVO

Dio 1. – Kaznena djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava

Članak 2. – NEZAKONITI PRISTUP

Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim

zakonodavstvom kaznenopravno sankcionirao namjerni čin neovlaštenog pristupanja cjelini ili dijelu računalnog sustava. Stranka može propisati da kazneno djelo mora biti počinjeno povredom sigurnosnih mjera s namjerom pribavljanja računalnih podataka ili s nekom drugom nepoštenom namjerom, ili u pogledu računalnog sustava koji je spojen s drugim računalnim sustavom.

Članak 3. – NEZAKONITO PRESRETANJE

Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni čin neovlaštenog presretanja nejavnih prijenosa računalnih podataka prema računalnom sustavu, iz njega ili unutar njega (uključujući i elektromagnetske emisije iz računalnog sustava koji prenosi te računalne podatke), počinjen tehničkim sredstvom. Stranka može propisati da kazneno djelo bude počinjeno s nepoštenom namjerom ili u pogledu računalnog sustava koji je spojen s drugim računalnim sustavom.

Članak 4. – OMETANJE PODATAKA

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni čin neovlaštenog oštećivanja, brisanja, kvarenja, mijenjanja ili činjenja neuporabljivima računalnih podataka.

2. Stranka može priuzdržati pravo propisati da ponašanjem opisanim u stavku 1. ovoga članka mora biti prouzročeno ozbiljno zlo.

Članak 5. – OMETANJE SUSTAVA

Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni čin ozbiljnog neovlaštenog sprječavanja funkcioniranja računalnog sustava unošenjem, prenošenjem, oštećivanjem, brisanjem, kvarenjem, mijenjanjem ili činjenjem neuporabljivima računalnih podataka.

Članak 6. – ZLOPORABA NAPRAVA

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni neovlašteni čin:

a. proizvodnje, prodaje, pribavljanja radi uporabe, uvoza, distribuiranja ili činjenja dostupnim na neki drugi način:

i. naprava, uključujući i računalne programe, stvorenih ili prilagođenih prvenstveno zbog svrhe počinjenja bilo kojeg od djela utvrđenih člancima 2.-5. ove Konvencije;

ii. računalne lozinke, pristupne šifre ili sličnog podatka, kojime bi se omogućilo pristupanje cjelini ili nekom dijelu računalnog sustava

s namjerom da bude upotrijebljen u svrhu počinjenja bilo kojeg od kaznenih djela utvrđenih člancima 2.-5. ove Konvencije i

b. posjedovanja neke od stvari navedenih u točki (a), alinejama 1. ili 2. ovoga članka s namjerom da bude upotrijebljena u svrhu počinjenja bilo kojeg od djela utvrđenih člancima 2.-5. stranka može zakonom uvjetovati da tek posjedovanje određenog broja takvih predmeta povlači kaznenu odgovornost.

2. Ovaj članak neće se tumačiti kao propisivanje kaznene odgovornosti u slučajevima kada proizvodnja, prodaja, pribavljanje radi uporabe, uvoz, distribuiranje, činjenje dostupnim na neki drugi način ili posjedovanje opisano u stavku 1. ovoga članka nije u svrhu počinjenja kaznenog djela propisanog člancima 2.-5. ove Konvencije, kao na primjer u slučaju ovlaštenog ispitivanja ili zaštite računalnog sustava.

3. Svaka stranka može pridržati pravo na neprimjenjivanje stavka 1. ovoga članka, uz uvjet da

rezerva ne obuhvaća prodaju, distribuciju ili činjenje dostupnim na neki drugi način predmeta navedenih u stavku 1. točki (a) alineji 2.

Dio 2. – Računalna kaznena djela

Članak 7. – RAČUNALNO KRIVOTVORENJE

Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni čin neovlaštenog unošenja, mijenjanja, brisanja ili činjenja neuporabljivima računalnih podataka, koji kao posljedicu ima nevjerodostojnost podataka, pri čemu postoji namjera da se oni u pravne svrhe smatraju vjerodostojnima, ili da se po njima postupa kao da su takvi, i to bez obzira jesu li ti podaci izravno čitljivi i razumljivi. Strana može propisati da tek postojanje prijevarne ili slične nepoštene namjere povlači kaznenu odgovornost.

Članak 8. – RAČUNALNA PRIJEVARA

Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni čin neovlaštenog uzrokovanja štete na imovini drugoga:

a. bilo kakvim unošenjem, mijenjanjem, brisanjem ili činjenjem neuporabljivima računalnih podataka,

b. bilo kakvim ometanjem funkcioniranja računalnog sustava

s prijevarnom ili nepoštenom namjerom neovlaštenog pribavljanja ekonomske koristi za sebe ili drugoga.

Dio 3. – Kaznena djela u svezi sa sadržajem

Članak 9. – KAZNENA DJELA VEZANA UZ DJEČJU PORNOGRAFIJU

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni neovlašteni čin:

a. proizvodnje dječje pornografije za svrhu njene distribucije putem računalnih sustava;

b. nuđenja ili činjenja dostupnim dječje pornografije putem računalnog sustava;

c. distribuiranja ili prenošenja dječje pornografije putem računalnog sustava;

d. pribavljanja dječje pornografije putem računalnog sustava za sebe ili drugoga;

e. posjedovanja dječje pornografije u računalnom sustavu ili na mediju za pohranu računalnih podataka.

2. U smislu stavka 1. ovoga članka izraz »dječja pornografija« uključuje pornografski materijal koji vizualno prikazuje:

a. maloljetnika kako sudjeluje u seksualno eksplicitnom ponašanju;

b. osobu koja izgleda kao maloljetnik koji sudjeluje u seksualno eksplicitnom ponašanju;

c. stvarne slike koje predstavljaju maloljetnika kako sudjeluje u seksualno eksplicitnom ponašanju.

3. U smislu stavka 2. ovoga članka, izraz »maloljetnik« uključuje sve osobe u dobi mlađoj od 18 godina. Međutim, stranka može utvrditi i nižu dobnu granicu, koja ne može biti ispod 16 godina starosti.

4. Svaka stranka može pridržati pravo neprimjenjivanja u cijelosti ili djelomice točaka (d) i (e) stavka 1., te točaka (b) i (c) stavka 2.

Dio 4. – Kaznena djela povrede autorskih i srodnih prava

Članak 10. – KAZNENA DJELA POVREDE AUTORSKIH I SRODNIH PRAVA

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirala povreda autorskog prava kako je ono utvrđeno po pravu te stranke, a u skladu s obvezama koje je stranka preuzela Pariškim aktom Bernske konvencije za zaštitu književnih i umjetničkih djela, Sporazumom o trgovinskim aspektima prava intelektualnog vlasništva i Ugovorom o autorskom pravu Svjetske organizacije za intelektualno vlasništvo (dalje u tekstu: WIPO), s izuzetkom svih moralnih prava priznatih tim konvencijama, i to kada do počinjenja dođe dragovoljno, u komercijalnim razmjerima i pomoću računalnog sustava.

2. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirala povreda srodnih prava kako su ona utvrđena po pravu te stranke, a u skladu s obvezama koje je stranka preuzela Međunarodnom konvencijom za zaštitu umjetnika izvođača, proizvođača fonograma i organizacija za radiodifuziju donesenom u Rimu (Rimska konvencija), Sporazumom o trgovinskim aspektima prava intelektualnog vlasništva i Ugovorom o izvedbama i fonogramima WIPO-a, izuzev svih moralnih prava priznatih tim konvencijama, i to kada do počinjenja dođe dragovoljno, u komercijalnim razmjerima i pomoću računalnog sustava.

3. Stranka može pridržavati pravo na nepropisivanje kaznene odgovornosti po stavcima 1. i 2. ovoga članka u ograničenim okolnostima, uz uvjet da su na raspolaganju druga učinkovita sredstva i da taj pridržaj ne umanjuje ili dokida međunarodne obveze stranke utvrđene međunarodnim dokumentima navedenim u stavcima 1. i 2. ovoga članka.

Dio 5. – Sporedna odgovornost i sankcije

Članak 11. – POKUŠAJ I POMAGANJE ILI POTICANJE

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni čin pomaganja ili poticanja na počinjenje bilo kojeg od kaznenih djela u skladu s člancima 2.–10. ove Konvencije s namjerom da to kazneno djelo bude počinjeno.

2. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se unutarnjim zakonodavstvom kaznenopravno sankcionirao namjerni čin pokušaja počinjenja bilo kojeg od kaznenih djela utvrđenih člancima 3.–5, 7., 8., te člankom 9. stavkom 1. točkom (c) ove Konvencije.

3. Svaka stranka može pridržati pravo neprimjenjivanja u cijelosti ili djelomice stavka 2. ovoga članka.

Članak 12. – ODGOVORNOST PRAVNIH OSOBA

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se osigurala mogućnost da pravna osoba bude pozvana na odgovornost za kaznena djela utvrđena ovom Konvencijom, koja je za njenu korist počinila neka fizička osoba, postupajući bilo samostalno ili kao dio tijela pravne osobe koji ima rukovodeće mjesto unutar pravne osobe, na temelju:

a. ovlaštenja za zastupanje pravne osobe;

b. ovlaštenja za donošenje odluka u ime pravne osobe;

c. rukovodećih ovlaštenja unutar pravne osobe.

2. Osim slučajeva predviđenih u stavku 1. ovoga članka, svaka stranka će poduzeti mjere potrebne kako bi se osigurala mogućnost da pravna osoba bude pozvana na odgovornost kada zbog nedostatka nadzora ili kontrole fizičke osobe iz stavka 1. ovoga članka, fizičkoj osobi koja

postupa po ovlaštenju i u korist pravne osobe bude omogućeno počinjenje kaznenog djela utvrđenog ovom Konvencijom.

3. U skladu s pravnim načelima stranke, odgovornost pravne osobe može biti kaznena, građanska ili upravna.

4. Ta odgovornost neće utjecati na kaznenu odgovornost fizičkih osoba koje su počinile djelo.

Članak 13. – SANKCIJE I MJERE

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se osiguralo da kaznena djela utvrđena člancima 2.–11. budu kažnjiva učinkovitim, srazmjernim i odgovarajućim sankcijama, koje uključuju i lišavanje slobode.

2. Svaka stranka će se pobrinuti da pravne osobe koje su utvrđene odgovornima temeljem članka 12. ove Konvencije budu podvrgnute učinkovitim, srazmjernim i odvraćajućim kaznenim ili nekaznenim sankcijama ili mjerama, uključujući i novčane kazne.

Odjeljak 2. – POSTUPOVNO PRAVO

Dio 1. – Opće odredbe

Članak 14. – PREDMET POSTUPOVNIH ODREDABA

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se uspostavila ovlaštenja i postupci utvrđeni ovim Odjeljkom u svrhu provedbe specifičnih kriminalističkih istraga i postupaka.

2. Osim ako je to izričito utvrđenom člankom 21., svaka stranka će ovlaštenja i postupke navedene u stavku 1. ovoga članka primjenjivati na:

a. kaznena djela utvrđena člancima 2.–11. ove Konvencije,

b. druga kaznena djela počinjena pomoću računalnog sustava i

c. prikupljanje dokaza o kaznenom djelu u elektroničkom obliku.

3. a. Svaka stranka može pridržati pravo primjenjivanja mjera navedenih u članku 20. samo na kaznena djela ili vrste kaznenih djela navedene u rezervi, uz uvjet da raspon tih kaznenih djela ili vrste kaznenih djela nije uži od raspona kaznenih djela na koja se primjenjuju mjere navedene u članku 21. Svaka stranka razmotrit će ograničavanje te rezerve kako bi se omogućila najširа moguća primjena mjere navedene u članku 20.

b. Kada stranka zbog ograničenja u svojem pozitivnom pravu u vrijeme usvajanja ove Konvencije nije u mogućnosti primijeniti mjere navedene u člancima 20. i 21. na komunikacije koje se prenose unutar računalnog sustava davatelja usluge, pri čemu:

i. se računalnim sustavom upravlja u korist zatvorene skupine korisnika, a

ii. računalni sustav ne koristi javne komunikacijske mreže i nije spojen s drugim računalnim sustavom, bilo javnim ili privatnim,

tada stranka u odnosu na takve komunikacije može pridržavati pravo neprimjenjivanja tih mjera. Svaka stranka će razmotriti ograničavanje te rezerve kako bi se omogućila najširа moguća primjena mjera navedenih u člancima 20. i 21.

Članak 15. – UVJETI I OČUVANJE LJUDSKIH PRAVA

1. Svaka stranka će se pobrinuti da uspostava, primjena i provedba ovlaštenja i postupaka utvrđenih ovim Odjeljkom bude u skladu s uvjetima i elementima očuvanja ljudskih prava utvrđenima unutarnjim pravom te stranke, što će omogućiti odgovarajuću zaštitu ljudskih prava i sloboda, uključujući i prava nastala u skladu s obvezama koje je stranka preuzela temeljem Konvencije Vijeća Europe o zaštiti prava i temeljnih sloboda čovjeka iz 1950. godine,

Međunarodnog pakta Ujedinjenih naroda o građanskim i političkim pravima iz 1966. godine, kao i temeljem drugih relevantnih međunarodnih sporazuma o ljudskim pravima, te u sebi sadržavati i načelo proporcionalnosti.

2. Ti će uvjeti i elementi očuvanja ljudskih prava, na odgovarajući način, u pogledu naravi konkretnog ovlaštenja ili postupka uključivati, među ostalim, sudski ili drugi nezavisni nadzor, provjeru osnova koje opravdavaju primjenu tog ovlaštenja ili postupka, kao i ograničenja njegovog opsega i trajanja.

3. Strana će, u opsegu sukladno javnim interesima, a naročito u interesu čvrste provedbe prava, razmotriti učinak koji ovlaštenja i postupci iz ovog Odjeljka imaju na prava, odgovornosti i legitimne interese trećih strana.

Dio 2. – Hitna zaštita pohranjenih računalnih podataka

Članak 16. – HITNA ZAŠTITA POHRANJENIH RAČUNALNIH PODATAKA

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela mogla naložiti, ili na drugi način postići, hitnu zaštitu određenih računalnih podataka, uključujući podatke o prometu koji su pohranjeni pomoću računalnog sustava, a naročito kada postoji osnova za sumnju da su računalni podaci osobito podložni mogućnosti uništenja ili mijenjanja.

2. Kada stranka provodi zaštitu iz stavka 1. ovoga članka izdavanjem naloga nekoj osobi da zaštiti određene pohranjene računalne podatke koje ta osoba posjeduje ili kontrolira, tada će stranka usvojiti zakonske i druge mjere potrebne kako bi se tu osobu obvezalo da te računalne podatke zaštiti i sačuva njihovu cjelovitost sve dok je to nužno, ali najviše 90 dana, kako bi nadležnim tijelima bilo omogućeno da zahtijevaju njihovo otkrivanje. Stranka može predvidjeti mogućnost naknadnog obnavljanja takvog naloga.

3. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se skrbnika ili drugu osobu koja čuva računalne podatke obvezalo da drži u tajnosti poduzimanje tih postupaka tijekom razdoblja koje je utvrđeno unutarnjim pravom stranke.

4. Ovlaštenja i postupci navedeni u ovom članku bit će u skladu s člancima 14. i 15. ove Konvencije.

Članak 17. – HITNA ZAŠTITA I DJELOMIČNO OTKRIVANJE PODATAKA O PROMETU

1. Svaka stranka će u pogledu podataka o prometu koje je potrebno zaštititi temeljem članka 16. usvojiti zakonske i druge mjere potrebne kako bi bilo osigurano:

a. da takva hitna zaštita podataka o prometu bude moguća bez obzira je li u prijenos te komunikacije bio uključen samo jedan ili više davatelja usluga; i

b. hitno otkrivanje nadležnom tijelu stranke, ili osobi koju to tijelo imenuje, dovoljne količine podataka o prometu kako bi bili identificirani davatelji usluga i put kojim je komunikacija prenesena.

2. Ovlaštenja i postupci navedeni u ovom članku bit će u skladu s člancima 14. i 15. ove Konvencije.

Dio 3. – Nalog za proizvodnju

Članak 18. – NALOG ZA PROIZVODNJU

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela bila ovlaštena naložiti:

a. osobi na državnom području stranke da dostavi određene računalne podatke koje ta osoba posjeduje ili kontrolira, a koji su pohranjeni u računalnom sustavu ili na mediju za pohranu računalnih podataka i

b. davatelju usluga koji svoje usluge nudi na državnom području stranke da dostavi pretplatničke informacije koje se odnose na te usluge, a koje informacije taj davatelj usluga posjeduje ili kontrolira.

2. Ovlaštenja i postupci navedeni u ovom članku bit će u skladu s člancima 14. i 15. ove Konvencije.

3. U smislu ovoga članka, izraz »pretplatničke informacije« označava sve informacije u obliku računalnog podatka ili u bilo kojem drugom obliku, koje ima davatelj usluga, a koje se tiču pretplatnika na njegove usluge, osim podataka o prometu ili sadržaju, a temeljem kojih informacija može biti utvrđeno sljedeće:

a. vrsta komunikacijske usluge koja je korištena, poduzete tehničke mjere i razdoblje pružanja usluge;

b. pretplatnikov identitet, poštanska ili zemljopisna adresa, broj telefona i drugi pristupni broj te informacije za slanje računa i informacije o plaćanju, raspoložive na osnovi pretplatničkog ugovora ili sporazuma;

c. sve druge informacije o mjestu gdje je komunikacijska oprema instalirana, raspoložive na osnovi pretplatničkog ugovora ili sporazuma.

Dio 4. – Pretraga i oduzimanje pohranjenih rčunalnih podataka

Članak 19. – PRETRAGA I ODUZIMANJE POHRANJENIH RAČUNALNIH PODATAKA

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela bila ovlaštena izvršiti pretragu ili na sličan način imali pristup:

a. računalnom sustavu ili njegovom dijelu, kao i računalnim podacima pohranjenim u njima;

b. mediju za pohranu računalnih podataka u kojemu računalni podaci mogu biti pohranjeni na državnom području stranke.

2. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se osiguralo da – u slučajevima kada njena tijela pretražuju ili na sličan način pristupaju određenom računalnom sustavu ili njegovom dijelu u skladu s točkom (a) stavka 1. ovoga članka, s osnovanom sumnjom da su traženi podaci pohranjeni u drugom računalnom sustavu ili njegovom dijelu na državnom području stranke, a tim se podacima može zakonito pristupiti iz prvog sutava, ili su njemu dostupni – ta tijela budu u mogućnosti hitno protegnuti pretragu ili slično postupanje i na taj drugi sustav.

3. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi ovlastila svoja nadležna tijela za oduzimanje ili osiguranje na neki sličan način računalnih podataka kojima je pristupljeno u skladu s odredbama stavaka 1. ili 2. ovoga članka. Te mjere će uključivati davanje ovlaštenja tijelima da:

a. oduzmu ili na sličan način osiguraju računalni sustav, njegov dio ili medij za pohranu računalnih podataka;

b. načine i zadrže kopiju tih računalnih podataka;

c. održe cjelovitost relevantnih pohranjenih računalnih podataka i

d. učine nepristupačnim ili odstrane te računalne podatke iz računalnog sustava kojemu je pristupljeno.

4. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela bila ovlaštena naložiti svakoj osobi koja ima saznanja o funkcioniranju računalnog sustava ili o mjerama poduzetim radi zaštite računalnih podataka u njemu da dade informacije koje su razumno nužne kako bi se omogućilo poduzimanje mjera navedenih u stavcima 1. i 2. ovoga članka.

5. Ovlaštenja i postupci navedeni u ovom članku bit će u skladu s člancima 14. i 15. ove Konvencije.

Dio 5. Prikupljanje računalnih podataka u realnom vremenu

Članak 20. – PRIKUPLJANJE RAČUNALNIH PODATAKA U REALNOM VREMENU

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela bila ovlaštena u realnom vremenu:

a. prikupiti ili snimiti primjenom tehničkih sredstava na državnom području te stranke, te

b. primorati davatelja usluga u okviru njegovih postojećih tehničkih mogućnosti da:

i. prikupi ili snimi primjenom tehničkih sredstava na državnom poručju te stranke ili

ii. surađuje i pomogne nadležnim tijelima da prikupe i snime

podatke o prometu u vezi s određenim komunikacijama na svojem državnom području prenesenima pomoću računalnog sustava.

2. Kada stranka zbog uspostavljenih načela svojega unutarnjeg pravnog sustava ne može usvojiti mjere navedene u točki (a) stavka 1., ona može umjesto toga usvojiti zakonske i druge mjere potrebne kako bi se osiguralo prikupljanje ili snimanje u realnom vremenu podataka o prometu vezanih uz određene komunikacije na njenom državnom području primjenom tehničkih sredstava na tom području.

3. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se davatelja usluga obvezalo da čuvaju u tajnosti činjenicu da je iskorišteno neko od ovlaštenja propisano ovim člankom, kao i sve informacije o tome.

4. Ovlaštenja i postupci navedeni u ovom članku bit će u skladu s člancima 14. i 15. ove Konvencije.

Članak 21. – PRESRETANJE PODATAKA O SADRŽAJU

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela, u odnosu na određena teška djela utvrđena unutarnjim pravom, bila ovlaštena u realnom vremenu:

a. prikupiti ili snimiti primjenom tehničkih sredstava na državnom području te stranke, te

b. primorati davtelja usluga u okviru njegovih postojećih tehničkih mogućnosti da:

i. prikupi ili snimi primjenom tehničkih sredstava na državnom području te stranke i

ii. surađuje i pomogne nadležnim tijelima da prikupe i snime

podatke o sadržaju u vezi s određenim komunikacijama na svojem državnom području prenesenima pomoću računalnog sustava.

2. Kada stranka zbog uspostavljenih načela svojega unutarnjeg pravnog sustava ne može usvojiti mjere navedene u točki (a) stavka 1., ona može umjesto toga usvojiti zakonske i druge mjere potrebne kako bi se osiguralo prikupljanje ili snimanje u realnom vremenu podataka o sadržaju podataka o navedenim komunikacijama na njenom državnom području kroz primjenu tehničkih sredstava na tom području.

3. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se davatelje usluga obvezalo da čuvaju u tajnosti činjenicu da je iskorišteno neko od ovlaštenja propisano ovim člankom, kao i sve informacije o tome.

4. Ovlaštenja i postupci navedeni u ovom članku bit će u skladu s člancima 14. i 15. ove Konvencije.

Odjeljak 3. – SUDBENOST

Članak 22. – SUDBENOST

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi uspostavila sudbenost za sva djela utvrđena člancima 2.–11. ove Konvencije, kada je djelo počinjeno:

a. na njenom državnom području; ili

b. na brodu koji vije zastavu te stranke, ili

c. u zrakoplovu registriranom po pravu te stranke, ili

d. od strane njenog državljanina, ako je djelo kažnjivo po kaznenom pravu mjesta gdje je počinjeno ili ako je djelo počinjeno izvan nadležnosti svih država.

2. Svaka država može pridržavati pravo neprimjenjivanja ili primjene samo u pojedinim slučajevima pravila o sudbenosti utvrđenih točkama (b),–(d). stavka (1) ovoga članka, ili nekim - njihovim dijelom.

3. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi uspostavila sudbenost za djela navedena u članku 24. stavku 1. ove Konvencije, i to u slučajevima kada je navodni počinitelj prisutan na njenom državnom području, a stranka ga po zahtjevu za izručenjem ne izručuje drugoj stranci isključivo na osnovi njegovog državljanstva.

4. Ova Konvencija ne isključuje nikakvu kaznenopravnu nadležnost izvršenu u skladu s domaćim pravom.

5. Kada jedna ili više stranaka zahtijevaju svoju sudbenost za navodno djelo utvrđeno odredbama ove Konvencije, tada će se stranke – kada je to moguće – posavjetovati s ciljem utvrđivanja najprikladnije sudbenosti za kazneni progon.

Poglavlje III. – MEĐUNARODNA SURADNJA

Odjeljak 1. – OPĆA NAČELA

Dio 1. – Opća načela međunarodne suradnje

Članak 23. – OPĆA NAČELA MEĐUNARODNE SURADNJE

Stranke će jedna s drugom surađivati u najširem mogućem opsegu u skladu s odredbama ovoga poglavlja, primjenjujući relevantne međunarodne instrumente međunarodne suradnje u kaznenopravnim stvarima, sporazume sklopljene na osnovi jedinstvenog ili recipročnog zakonodavstva i unutarnjeg prava, u svrhu provođenja istraga i postupaka povodom kaznenih djela vezanih uz računalne sustave i podatke ili u svrhu prikupljanja dokaza o kaznenom djelu u elektroničkom obliku.

Dio 2. – Načela izručenja

Članak 24. – IZRUČENJE

1. a. Ovaj članak primjenjuje se na izručenje između stranaka zbog kaznenih djela utvrđenih člancima 2.–11. ove Konvencije, uz uvjet da su po pravima obiju stranaka ta djela kažnjiva oduzimanjem slobode u trajanju od najmanje jedne godine ili težom kaznom.

b. Kada su u primjeni između dviju stranaka sporazum sklopljen na osnovi jedinstvenog ili recipročnog prava i ugovor o izručenju – uključujući i Europsku konvenciju o izručenju (ETS br. 24.) – koji predviđaju različite najmanje kazne, bit će primijenjena najmanja kazna propisana tim sporazumima ili ugovorima.

2. Kaznena djela opisana u stavku 1. ovoga članka smatrat će se kaznenim djelima prikladnima za izručenje po bilo kojem ugovoru o izručenju koji postoji između stranaka. Stranke se obvezuju u sve ugovore o izručenju koji budu zaključeni između stranaka uvrstiti ta djela među djela prikladna za izručenje.

3. Ako stranka koja uvjetuje izručenje postojanjem međunarodnog ugovora primi zahtjev za

izručenjem od druge stranke s kojom nema ugovor o izručenju, stranka koja izručuje može smatrati ovu Konvenciju pravnom osnovom za izručenje u pogledu svih kaznenih djela navedenih u stavku 1. ovoga članka.

4. Stranke koje uvjetuju izručenje postojanjem međunarodnog ugovora smatrat će kaznena djela navedena u stavku 1. ovoga članka prikladnim za izručenje među sobom.

5. Izručenje podliježe uvjetima utvrđenim pravom stranke primateljice zahtjeva za izručenjem ili mjerodavnim međunarodnim ugovorima o izručenju, uključujući i osnove po kojima stranka primateljica zahtjeva za izručenjem može odbiti izručenje.

6. Ako je izručenje zbog kaznenog djela navedenog u stavku 1. ovoga članka odbijeno isključivo na osnovi državljanstva osobe čije se izručenje traži, ili zbog toga što stranka primateljica zahtjeva drži da ona ima sudbenost nad tim djelom, stranka primateljica zahtjeva dostavit će taj slučaj, na zahtjev stranke pošiljateljice zahtjeva, svojim nadležnim tijelima u svrhu progona, te će stranku pošiljateljicu zahtjeva pravodobno izvijestiti o konačnom ishodu. Ta će tijela donijeti svoju odluku i provesti svoje istražne radnje i postupke na isti način kao i u slučaju svakog drugog djela usporedive naravi po pravu te stranke.

7. a. Svaka stranka će u vrijeme potpisivanja ili polaganja svojih isprava o ratifikaciji, prihvatu, odobrenju ili pristupu dostaviti Glavnom tajniku Vijeća Europe nazive i adrese svakog tijela odgovornog za podnošenje ili primanje zahtjeva za izručenje ili za zadržavanje u pritvoru u slučaju nepostojanja međunarodnog ugovora.

b. Glavni tajnik Vijeća Europe osnovat će i održavati ažurnim registar tijela koje su stranke odredile na ovaj način. Svaka stranka će se pobrinuti da pojedinosti upisane u registar budu u svako doba točne.

Dio 3. – Opća načela uzajamne pomoći

Članak 25. – OPĆA NAČELA UZAJAMNE POMOĆI

1. Stranke će jedna drugoj pružiti uzajamnu pomoć u najširem mogućem opsegu u svrhu provođenja istraga ili postupaka povodom kaznenih djela vezanih uz računalne sustave i podatke, ili u svrhu prikupljanja dokaza o kaznenom djelu u elektroničkom obliku.

2. Svaka stranka će također usvojiti zakonske i druge mjere potrebne kako bi izvršila obveze utvrđene člancima 27.-35. ove Konvencije.

3. Svaka stranka može u hitnim okolnostima postavljati zahtjeve za uzajamnom pomoći ili slati komunikacije s time u vezi koristeći se hitnim sredstvima komuniciranja (uključujući telefaks ili elektroničku poštu) u opsegu u kojem ta sredstva komuniciranja osiguravaju odgovarajuću razinu sigurnosti i vjerodostojnosti (uključujući i uporabu kriptiranja u slučaju potrebe), te uz kasniju formalnu potvrdu ukoliko to traži stranka primateljica zahtjeva. Stranka primateljica prihvatit će i odgovoriti na zahtjev postavljen putem bilo kojega od tih hitnih sredstava komunikacije.

4. Osim ako je člancima ovog poglavlja utvrđeno drugačije, uzajamna pomoć podliježe uvjetima utvrđenim pravom stranke primateljice zahtjeva ili merodavnim ugovorima o uzajamnoj pomoći, uključujući i osnove po kojima stranka primateljica zahtjeva može odbiti suradnju. Stranka primateljica zahtjeva neće iskoristiti pravo na odbijanje uzajamne pomoći u pogledu djela navedenih u člancima 2.-11. isključivo na osnovi toga što se zahtjev odnosi na djelo koje stranka primateljica zahtjeva smatra fiskalnim djelom.

5. Kada stranka primateljica zahtjeva u skladu s odredbama ovoga poglavlja smije uvjetovati pružanje uzajamne pomoći postojanjem dvojne kaznene odgovornosti, taj će se uvjet smatrati

ispunjenim – ako se ponašanje koje tvori djelo u pogledu kojega se traži pomoć smatra kaznenim djelom po pravima obiju stranaka – i bez obzira na činjenicu kategorizira li pravo stranke primateljice zahtjeva to djelo jednako kao i pravo stranke pošiljateljice zahtjeva, te bez obzira naziva li ga istom terminologijom.

Članak 26. SPONTANE INFORMACIJE

1. Stranka može u granicama svojeg unutarnjeg prava i bez prethodnog zahtjeva proslijediti drugoj stranci informacije dobivene u sklopu svojih vlastitih istraga, kada smatra da otkrivanje tih informacija može pomoći stranci primateljici pri pokretanju ili vođenju istraga ili postupaka povodom kaznenih djela utvrđenih ovom Konvencijom, ili kada smatra da to može dovesti do zahtjeva te stranke za suradnjom u skladu s odredbama ovoga poglavlja.

2. Prije davanja tih informacija stranka davateljica može zatražiti da oni ostanu tajni ili da budu upotrijebljeni pod određenim uvjetima. Ako stranka primateljica ne može udovoljiti tom zahtjevu, o tome će obavijestiti stranku davateljicu, koja će tada odlučiti hoće li i unatoč tome dati te informacije. Ako stranka primateljica prihvati informacije pod određenim uvjetima, obvezna ih je poštivati.

Dio 4. – Postupci vezani uz zahtjeve za uzajamnom pomoći u slučaju nepostojanja mjerodavnih međunarodnih ugovora

Članak 27. – POSTUPCI VEZANI UZ ZAHTJEVE ZA UZAJAMNOM POMOĆI U SLUČAJU NEPOSTOJANJA MJERODAVNIH MEĐUNARODNIH UGOVORA

1. U slučaju kada između stranke pošiljateljice i primateljice zahtjeva nije na snazi nikakav ugovor o uzajamnoj pomoći na osnovi jedinstvenog ili recipročnog prava, primjenjivat će se odredbe stavaka 2.-9. ovoga članka. Kada takav međunarodni ugovor, sporazum ili propis postoji, odredbe ovoga članka neće se primjenjivati osim ako umjesto njihove primjene stranke ugovore primjenu neke ili sve niže navedenih odredbe ovoga članka.

2. a. Svaka stranka će odrediti središnje tijelo ili tijela odgovorna za slanje i odgovaranje na zahtjeve za pružanjem uzajamne pomoći, za izvršavanje tih zahtjeva ili njihovo prosljeđivanje tijelima nadležnim za njihovu provedbu.

b. Središnja tijela će komunicirati izravno jedan s drugime.

c. Svaka stranka će u vrijeme potpisivanja ili polaganja svojih isprava o ratifikaciji, prihvatu, odobrenju ili pristupu dostaviti Glavnom tajniku Vijeća Europe nazive i adrese tijela koje je odredila postupajući po odredbama ovoga stavka.

d. Glavni tajnik Vijeća Europe osnovat će i održavati ažurnim registar središnjih tijela koje su stranke na ovaj način odredile. Svaka stranka će se pobrinuti da pojedinosti upisane u registar budu u svako doba točne.

3. Zahtjevi za uzajamnom pomoći po ovom članku bit će izvršeni u skladu s postupcima koje odredi stranka pošiljateljica zahtjeva, osim kada to nije u neskladu s pravom stranke primateljice zahtjeva.

4. osim s osnova za odbijanje utvrđenih člankom 25. stavkom 4., stranka primateljica zahtjeva može odbiti pružiti pomoć ako:

a. se zahtjev odnosi na djelo koje stranka primateljica smatra političkim djelom ili djelom povezanim s političkim djelom, ili

b. smatra da će izvršenje zahtjeva vjerojatno ugroziti njen suverenitet, sigurnost, javni poredak ili druge bitne interese.

5. Stranka primateljica može odgoditi postupanje po zahtjevu ako bi to postupanje ugrozilo

kaznene istrage ili postupke koje vode njezina tijela.

6. Prije odbijanja ili odgađanja pružanja pomoći stranka primateljica će – kada je to prikladno i nakon savjetovanja sa strankom pošiljateljicom – razmotriti može li zahtjevu biti udovoljeno djelomično ili pod onim uvjetima koje stranka primateljica smatra nužnima.

7. Stranka primateljica će bez odgađanja izvijestiti stranku pošiljateljicu o ishodu izvršenja zahtjeva za pružanjem pomoći. Ako je zahtjev odbijen ili odgođen, dat će razloge za odbijanje ili odgodu. Stranka primateljica će također izvijestiti stranku pošiljateljicu o svim razlozima koji čine nemogućim izvršavanje zahtjeva, ili će ga vjerojatno znatno odgoditi.

8. Stranka pošiljateljica može od stranke primateljice zahtijevati da zadrži u tajnosti činjenicu da je u skladu s odredbama ovoga poglavlja postavljen zahtjev, kao i njegov sadržaj, osim utoliko koliko je nužno za izvršavanje zahtjeva. Ako stranka primateljica ne može udovoljiti tom zahtjevu za tajnošću, o tome će bez odgađanja obavijestiti stranku pošiljateljicu, koja će tada odlučiti treba li i unatoč tome zahtjev biti izvršen.

9. a. U slučaju hitnosti pravosudnim tijelima stranke pošiljateljice mogu slati zahtjeve za uzajamnom pomoći i komunikacije u vezi s njima izravno odgovarajućim tijelima stranke primateljice. U svakom takvom slučaju jedan primjerak će istodobno biti poslan i središnjem tijelu stranke primateljice putem središnjeg tijela stranke pošiljateljice.

b. Svaki zahtjev ili komunikacija po ovom stavku mogu biti upućeni putem Međunarodne organizacije kriminalističke policije (International Criminal Police Organisation – Interpol).

c. Kada je zahtjev upućen u skladu s točkom (a) ovoga stavka, a tijelo nije nadležno za postupanje po zahtjevu, ono će zahtjev uputiti nadležnom nacionalnom tijelu i izravno izvijestiti stranku pošiljateljicu da je tako postupio.

d. Nadležno tijelo stranke pošiljateljice može zahtjeve i komunikacije upućene u skladu s ovim stavkom koji ne uključuju prisilne mjere dostaviti izravno nadležnim tijelima stranke primateljice.

e. Svaka stranka može u vrijeme potpisivanja ili polaganja svoje isprave o ratifikaciji, prihvatu, odobrenju ili pristupu izvijestiti Glavnog tajnika Vijeća Europe da iz razloga učinkovitosti zahtjeve upućene temeljem ovoga stavka treba uputiti njenom središnjem tijelu.

Članak 28. – TAJNOST I OGRANIČENJE KORIŠTENJA

1. U slučajevima kada između stranke pošiljateljice i stranke primateljice zahtjeva nije na snazi nikakav ugovor o uzajamnoj pomoći na osnovi jedinstvenog ili recipročnog prava, primjenjivat će se odredbe ovoga članka. Kada takav međunarodni ugovor, sporazum ili propis postoji, odredbe ovoga članka neće se primjenjivati, osim ako umjesto njihove primjene stranke ne ugovore primjenu neke ili sviju niže navedenih odredaba ovoga članka.

2. Stranka primateljica može pri odgovaranju na zahtjev uvjetovati dostavljanje informacija ili materijala time da oni:

a. budu držani u tajnosti, ako zahtjevu za uzajamnom pravom pomoći nije moglo biti udovoljeno zbog nepostojanja tog uvjeta; ili

b. ne budu korišteni za neke druge istrage ili postupke, osim onih navedenih u zahtjevu.

3. Ako stranka pošiljateljica ne može udovoljiti uvjetu navedenom u stavku 2. ovoga članka, o tome će obavijestiti drugu stranku, koja će tada odlučiti hoće li i unatoč tome dati te informacije. Ako stranka pošiljateljica prihvati taj uvjet, obvezna ga je poštivati.

4. Svaka stranka koja dostavlja informacije ili materijal pod uvjetom navedenim u stavku 2. ovoga članka može od druge stranke zatražiti da – u vezi s tim uvjetom – objasni korist od te

informacije ili materijala.

Odjeljak 2. – POSEBNE ODREDBE

Dio 1. – Uzajamna pomoć u pogledu privremenih mjera

Članak 29. – HITNA ZAŠTITA POHRANJENIH RAČUNALNIH PODATAKA

1. Stranka može od druge stranke zatražiti da naloži ili da na drugi način osigura hitnu zaštitu podataka pohranjenih pomoću računalnog sustava koji je smješten na državnom području stranke primateljice, a u pogledu kojega stranka pošiljateljica namjerava postaviti zahtjev za uzajamnom pomoći putem pretrage ili sličnog načina pristupa, oduzimanjem ili sličnim osiguranjem ili otkrivanjem podataka.

2. U zahtjevu za zaštitom temeljem stavka 1. ovoga članka bit će naznačene sljedeće pojedinosti:

a. tijelo koje zahtijeva zaštitu;

b. djelo koje je predmetom kriminalističke istrage ili postupka i kratak sažetak s tim povezanih činjenica;

c. pohranjene računalne podatke koje treba zaštititi i njihovu povezanost s djelom;

d. sve dostupne informacije za identifikaciju skrbnika pohranjenih računalnih podataka ili mjesto gdje se računalni sustav nalazi;

e. nužnost zaštite;

f. da stranka namjerava podnijeti zahtjev za uzajamnom pomoći putem pretrage ili sličnog načina pristupa, oduzimanjem ili sličnim osiguranjem ili otkrivanjem pohranjenih računalnih podataka.

3. Nakon primitka zahtjeva druge stranke, stranka primateljica će poduzeti sve odgovarajuće mjere kako bi hitno zaštitila naznačene podatke u skladu sa svojim unutarnjim pravom. U svrhu odgovaranja na zahtjev, dvojna kaznena odgovornost neće biti potrebna kao preduvjet za provedbu zaštite.

4. Stranka koja dvojnom kaznenom odgovornošću uvjetuje odgovor na zahtjev za uzajamnom pomoći putem pretrage ili sličnog načina pristupa, oduzimanjem, osiguranjem ili otkrivanjem podataka, može u pogledu ostalih djela – osim onih utvrđenih člancima 2.-11. ove Konvencije – pridržati pravo odbiti zahtjev za zaštitom po ovom članku u slučajevima kada ima razloga vjerovati da u trenutku otkrivanja uvjet dvojne kaznene odgovornosti ne može biti ispunjen.

5. Nadalje, zahtjev za zaštitom može biti odbijen jedino ako:

a. se zahtjev odnosi na djelo koje stranka primateljica smatra političkim djelom ili djelom povezanim s političkim djelom, ili

b. stranka primateljica smatra da će izvršenje zahtjeva vjerojatno ugroziti njen suverenitet, sigurnost, javni poredak ili druge bitne interese.

6. Kada stranka primateljica vjeruje da zaštita neće osigurati buduću dostupnost podataka ili da će predstavljati opasnost za tajnost ili na drugi način ugroziti istragu koju provodi stranka pošiljateljica, bez odgađanja će o tome izvijestiti stranku pošiljateljicu, koja će tada odlučiti treba li i unatoč tome zahtjev biti izvršen.

7. Svaka zaštita izvršena kao odgovor na zahtjev naveden u stavku 1. ovoga članka trajat će najmanje 60 dana, kako bi stranci pošiljateljici bilo omogućeno da podnese zahtjev za pretragu ili sličan način pristupa, oduzimanje ili slično osiguranje ili otkrivanje podataka. Nakon primitka takvog zahtjeva, nastavit će se sa zaštitom podataka do donošenja odluke o tom zahtjevu.

Članak 30. – HITNO OTKRIVANJE ZAŠTIĆENIH PODATAKA O PROMETU

1. Kada tijekom izvršavanja zahtjeva za zaštitom podataka o prometu koji se odnose na određenu komunikaciju, postavljenog u skladu s člankom 29., stranka primateljica zahtjeva da joj se otkrije da je davatelj usluga u nekoj drugoj državi bio upleten u prenošenje te komunikacije, stranka primateljica će hitno otkriti stranci pošiljateljici onu količinu podataka o prometu koja je dovoljna kako bi bila identificirani davatelj usluga i put kojim je komunikacija prenesena.

2. Otkrivanje podataka o prometu temeljem stavka 1. ovoga članka može biti uskraćeno jedino ako:

a. se zahtjev odnosi na djelo koje stranka primateljica smatra političkim djelom ili djelom povezanim s političkim djelom, ili

b. stranka primateljica smatra da će izvršenje zahtjeva vjerojatno ugroziti njen suverenitet, sigurnost, javni poredak ili druge bitne interese.

Dio 2. – Uzajamna pomoć glede istražnih ovlaštenja

Članak 31. – UZAJAMNA POMOĆ GLEDE PRISTU-PANJA POHRANJENIM RAČUNALNIM PODACIMA

1. Stranka može zatražiti od druge stranke da pretraži ili na sličan način pristupi, oduzme ili na sličan način osigura i otkrije podatke pohranjene pomoću računalnog sustava smještenog unutar državnom području stranke primateljice zahtjeva, uključujući i podatke zaštićene u skladu s odredbama članka 29. ove Konvencije.

2. Stranka primateljica zahtjeva će odgovoriti na zahtjev primjenom međunarodnih instrumenata, sporazuma i propisa navedenih u članku 23., te sukladno ostalim relevantnim odredbama ovoga poglavlja.

3. Odgovor na zahtjev će biti hitan kada:

a. postoji osnova za sumnju da su računalni podaci osobito podložni mogućnosti uništenja ili mijenjanja ili

b. instrumenti, sporazumi i propisi navedeni u stavku 2. ovoga članka i inače određuju hitnu suradnju.

Članak 32. – PREKOGRANIČNO PRISTUPANJE POHRANJENIM RAČUNALNIM PODACIMA UZ SUGLASNOST ILI U SLUČAJU JAVNE DOSTUPNOSTI

Stranka može bez pribavljanja odobrenja druge stranke:

a. pristupiti javno dostupnim (»open source«) pohranjenim računalnim podacima, bez obzira gdje su zemljopisno smješteni ili

b. pristupiti ili primati putem računalnog sustava na svojem državnom području pohranjene računalne podatke smještene u drugoj stranci, ako stranka dobije zakonitu i dragovoljnu suglasnost osobe koja ima zakonito ovlaštenje otkrivati podatke stranci pomoću tog računalnog sustava.

Članak 33. – UZAJAMNA POMOĆ GLEDE PRIKUPLJANJA PODATAKA O PROMETU U REALNOM VREMENU

1. Stranke će jedna drugoj pružiti uzajamnu pomoć u pogledu prikupljanja u realnom vremenu podataka o prometu vezanih uz određene komunikacije na svojem državnom području koje su prenesene pomoću računalnog sustava. U skladu s odredbama stavka 2. ovoga članka, za pomoć će biti mjerodavni uvjeti i postupci utvrđeni unutarnjim pravom.

2. Svaka stranka će takvu pomoć pružiti barem u pogledu kaznenih djela kod kojih je u

sličnim domaćim slučajevima moguće u realnom vremenu prikupiti podatke o prometu.

Članak 34. – UZAJAMNA POMOĆ U ODNOSU NA PRESRETANJE PODATAKA O SADRŽAJU

Stranke će jedna drugoj pružati uzajamnu pomoć u pogledu prikupljanja ili snimanja u realnom vremenu podataka o sadržaju određenih komunikacija prenesenih pomoću računalnog sustava, i to u opsegu dozvoljenom njihovim mjerodavnim međunarodnim ugovorima i unutarnjim pravom.

Dio 3. – Mreža u neprekidnom pogonu

Članak 35. – MREŽA U NEPREKIDNOM POGONU

1. Svaka stranka će odrediti kontaktno mjesto dostupno od 0 do 24 sata, 7 dana u tjednu, kako bi osigurala pružanje trenutne pomoći u svrhu istraga i postupaka povodom kaznenih djela vezanih uz računalne sustave i podatke, kao i u svrhu prikupljanja dokaza o kaznenom djelu u elektroničkom obliku. Takva će pomoć obuhvaćati omogućavanje ili – ako je to dopušteno unutarnjim pravom i pravnom praksom – izravno izvršavanje:

a. davanja tehničkih savjeta;

b. zaštite podataka u skladu s odredbama članka 29. i 30. i

c. prikupljanja dokaza, davanja pravnih informacija i lociranja osumnjičenika.

2. a. Kontaktno mjesto stranke imat će mogućnost i ovlaštenje hitno komunicirati s kontaktnim mjestom druge stranke.

b. Ako kontaktno mjesto koje je stranka odredila nije dio tijela te stranke zaduženog ili zaduženih za međunarodnu uzajamnu pomoć ili izručenje, tada će kontaktno mjesto morati biti u stanju hitno koordinirati svoje aktivnosti s tim organom ili organima.

3. Kako bi rad mreže bio olakšan, svaka stranka će osigurati da na raspolaganju bude obučeno i opremljeno osoblje.

Poglavlje IV. – ZAVRŠNE ODREDBE

Članak 36. – POTPISIVANJE I STUPANJE NA SNAGU

1. Ova Konvencija bit će otvorena za potpisivanje državama članicama Vijeća Europe i državama nečlanicama koje su sudjelovale u njezinoj izradi.

2. Ova Konvencija podliježe ratifikaciji, prihvatu, odobrenju ili pristupu. Isprave o ratifikaciji, prihvatu, odobrenju ili pristupu bit će položene kod Glavnog tajnika Vijeća Europe.

3. Ova Konvencija stupa na snagu prvoga dana u mjesecu nakon isteka razdoblja od tri mjeseca nakon dana na koji je pet država, od kojih su najmanje tri države članice Vijeća Europe, izrazilo svoj pristanak da budu vezane ovom Konvencijom u skladu s odredbama stavaka 1. i 2. ovoga članka.

4. U odnosu na svaku državu potpisnicu koja naknadno izrazi svoj pristanak da bude vezana ovom Konvencijom, ista stupa na snagu prvoga dana u mjesecu nakon isteka razdoblja od tri mjeseca nakon dana izražavanja tog pristanka u skladu s odredbama stavaka 1. i 2. ovoga članka.

Članak 37. – PRISTUPANJE KONVENCIJI

1. Nakon stupanja na snagu ove Konvencije, Odbor ministara Vijeća Europe, nakon savjetovanja s državama ugovornicama ove Konvencije, može pozvati na pristupanje bilo koju državu nečlanicu Vijeća koja nije sudjelovala u njenoj izradi. Odluka o tome će biti donesena većinom utvrđenom člankom 20. d Statuta Vijeća Europe i jednoglasnom odlukom predstavnika

država ugovornica zastupljenih u Odboru ministara.

2. U odnosu na bilo koju državu koja pristupa Konvenciji u skladu s odredbama stavka 1. ovoga članka, ista stupa na snagu prvoga dana u mjesecu nakon isteka razdoblja od tri mjeseca nakon dana polaganja isprave o ratifikaciji, prihvatu, odobrenju ili pristupu kod Glavnog tajnika Vijeća Europe.

Članak 38. – TERITORIJALNA PRIMJENA

1. Bilo koja država može u vrijeme potpisivanja ili polaganja svoje isprave o ratifikaciji, prihvatu, odobrenju ili pristupu odrediti neko područje ili više njih, na koje se primjenjuje ova Konvencija.

2. Bilo koja stranka može u nekom kasnijem trenutku izjavom upućenom Glavnom tajniku Vijeća Europe proširiti teritorijalnu primjenu ove Konvencije na neko drugo područje kojega je navela u toj izjavi. U pogledu tog područja ova Konvencija stupa na snagu prvoga dana u mjesecu nakon isteka razdoblja od tri mjeseca nakon dana kada Glavni tajnik Vijeća Europe primi tu izjavu.

3. Svaka izjava dana u skladu s odredbama prethodnih dvaju stavaka može u odnosu na područje navedeno u toj izjavi biti povučena putem notifikacije upućene Glavnom tajniku Vijeća Europe. Povlačenje stupa na snagu prvoga dana u mjesecu nakon isteka razdoblja od tri mjeseca nakon dana kada Glavni tajnik Vijeća Europe primi tu notifikaciju.

Članak 39. – UČINCI KONVENCIJE

1. Svrha je ove Konvencije dopuniti mjerodavne višestrane ili dvostrane međunarodne ugovore ili sporazume između stranaka, uključujući i odredbe:

– Europske konvencije o izručenju, otvorene za potpisivanje u Parizu dne. 13. prosinca 1957. godine (ETS br. 24);

– Europske konvencije o uzajamnoj pomoći u kaznenim predmetima, otvorene za potpisivanje u Strasbourgu dne. 20. travnja 1959. godine (ETS br. 30);

– Dopunskog protokola Europskoj konvenciji o uzajamnoj pomoći u kaznenim predmetima, otvorenoga za potpisivanje u Strasbourgu dne. 17. ožujka 1978. godine (ETS br. 99).

2. Ako su dvije ili više stranaka već zaključile sporazum ili međunarodni ugovor o predmetima koje uređuje ova Konvencija, ili ako su na neki drugi način uspostavile međusobne odnose u tim stvarima, ili ako u budućnosti to namjeravaju učiniti, one će biti ovlaštene primjenjivati i taj sporazum ili međunarodni ugovor, kao i urediti te odnose s time u skladu. Međutim, kada u pogledu predmeta koje uređuje ova Konvencija stranke uspostave svoje odnose na način različit od uređenja predviđenog ovom Konvencijom, stranke će to učiniti na način koji nije u neskladu s ciljevima i načelima ove Konvencije.

3. Sadržaj ove Konvencije neće utjecati na ostala prava, ograničenja, obveze i odgovornosti stranaka.

Članak 40. – IZJAVE

Pisanom notifikacijom upućenom Glavnom tajniku Vijeća Europe sve države mogu u vrijeme potpisivanja ili polaganja svoje isprave o ratifikaciji, prihvatu, odobrenju ili pristupu izjaviti da će se poslužiti mogućnošću da zahtijevaju dodatne elemente utvrđene člancima 2. i 3., člankom 6. stavkom 1. točkom (b), člankom 7., člankom 9. stavkom 3. i člankom 27. stavkom 9. točkom (e).

Članak 41. – FEDERALNA KLAUZULA

1. Savezna država može pridržati pravo preuzeti obveze po poglavlju II. ove Konvencije u

skladu sa svojim temeljnim načelima koja uređuju odnose između središnjih vlasti i saveznih država ili drugih sličnih teritorijalnih jedinica, uz uvjet da je ta država ipak u mogućnosti surađivati u skladu s odredbama poglavlja III. ove Konvencije.

2. Prilikom izražavanja rezerve u skladu sa stavkom 1. ovoga članka, savezna država ne može uvjete te rezerve primijeniti na način da isključi ili bitno umanji svoje obveze da se pobrine za mjere utvrđene poglavljem II. ove Konvencije. Ta će se država, ukupno gledajući, pobrinuti za mogućnost široke i učinkovite zakonske provedbe u pogledu tih mjera.

3. U pogledu odredaba ove Konvencije čija primjena spada u nadležnost saveznih država ili drugih sličnih federalnih teritorijalnih jedinica koje temeljem ustavnog uređenja nisu obvezne poduzimati zakonodavne mjere, savezna vlada će izvijestiti nadležna tijela saveznih država o navedenim odredbama, izražavajući pritom svoje povoljno mišljenje o istima, te potičući tijela saveznih država na poduzimanje odgovarajućih postupaka kako bi te odredbe stupile na snagu.

Članak 42. – REZERVE

Pisanom notifikacijom upućenom Glavnom tajniku Vijeća Europe sve države mogu u vrijeme potpisivanja ili polaganja svojih isprava o ratifikaciji, prihvatu, odobrenju ili pristupu izjaviti da će se poslužiti mogućnošću izjavljivanja rezervi omogućenih člankom 4. stavkom 2., člankom 6., stavkom 3., člankom 9. stavkom 4., člankom 10. stavkom 3., člankom 11. stavkom 3., člankom 14. stavkom 3., člankom 22. stavkom 2., člankom 29. stavkom 4. i člankom 41. stavkom 1. Niti jedna druga rezerva ne može biti izjavljena.

Članak 43. – STATUS I POVLAČENJE REZERVE

1. Stranka koja je izjavila rezervu u skladu s člankom 42. može tu rezervu u cijelosti ili djelomice povući notifikacijom upućenom Glavnom tajniku. To će povlačenje stupiti na snagu danom kada ga je Glavni tajnik Vijeća Europe primio. Ako notifikacija utvrđuje da povlačenje rezerve stupa na snagu na dan utvrđen u samoj notifikaciji, a taj dan pada nakon dana kada je Glavni tajnik primio notifikaciju, povlačenje će stupiti na snagu na taj kasniji dan.

2. Stranka koja je izjavila rezervu kako je navedeno u članku 42. povući će tu rezervu u cijelosti ili djelomice što prije okolnosti to dopuste.

3. Glavni tajnik Vijeća Europe može stranke koje su u skladu s člankom 42. izjavile jednu ili više rezervi periodički ispitivati o izgledima za povlačenje tih rezervi.

Članak 44. – IZMJENE I DOPUNE

1. Bilo koja od stranaka može uputiti prijedlog izmjena ili dopuna ove Konvencije. Taj će prijedlog Glavni tajnik Vijeća Europe dostaviti državama članicama Vijeća Europe, državama nečlanicama koje su sudjelovale u izradi ove Konvencije, kao i svakoj državi koja joj je pristupila ili je bila pozvana da joj pristupi u skladu s odredbama članka 37.

2. Svaka izmjena ili dopuna koju predloži stranka bit će dostavljena Europskom odboru za probleme kriminaliteta (CDPC), koji će Odboru ministara podnijeti svoje mišljenje o predloženoj izmjeni ili dopuni.

3. Odbor ministara će razmotriti predloženu izmjenu ili dopunu i mišljenje kojega je podnio Europski odbor za probleme kriminaliteta (CDPC). Nakon savjetovanja s državama nečlanicama strankama ove Konvencije. Odbor ministara može usvojiti izmjenu ili dopunu.

4. Tekst bilo koje izmjene ili dopune kojega usvoji Odbor ministara u skladu sa stavkom 3. ovoga članka bit će proslijeđen strankama na prihvaćanje.

5. Bilo koja izmjena ili dopuna usvojena u skladu sa stavkom 3. ovoga članka stupit će na

snagu tridesetog dana nakon dana kada sve stranke izvijeste Glavnog tajnika o svojem prihvaćanju iste.

Članak 45. – RJEŠAVANJE SPOROVA

1. Europski odbor za probleme kriminaliteta (CDPC) će biti izvještavan o tumačenju i provedbi ove Konvencije.

2. U slučaju spora između stranaka u pogledu tumačenja ili provedbe ove Konvencije, stranke će pokušati riješiti spor pregovorima ili nekim drugim miroljubivim načinom po vlastitom izboru, uključujući i podnošenje spora Europskom odboru za probleme kriminaliteta (CDPC), nekom arbitražnom sudu čije će odluke biti obvezujuće za stranke, ili Međunarodnom sudu pravde, ako se o tome sporazumiju stranke u sporu.

Članak 46. – SAVJETOVANJE STRANAKA

1. Stranke će se, kada to bude prikladno, periodički savjetovati s ciljem omogućavanja:

a. učinkovite uporabe i primjene ove Konvencije, uključujući i identifikaciju svih problema pri tome, kao i o učincima bilo koje izjave ili rezerve, izjavljene temeljem ove Konvencije;

b. razmjene informacija o značajnim pravnim, političkim ili tehnološkim događanjima vezanim uz kibernetički kriminal i prikupljanje dokaza u elektroničkom obliku;

c. razmatranja mogućeg dopunjavanja ili mijenjanja ove Konvencije.

2. Europski odbor za probleme kriminaliteta (CDPC) će biti periodički izvještavan o rezultatu savjetovanja iz stavka 1. ovoga članka.

3. Europski odbor za probleme kriminaliteta (CDPC) će, kada to bude prikladno, omogućiti savjetovanje iz stavka 1. ovoga članka, te će poduzeti mjere potrebne kako bi pomogao strankama u njihovim naporima da dopune ili izmijene ovu Konvenciju. Najkasnije tri godine nakon stupanja na snagu ove Konvencije Europski odbor za probleme kriminaliteta (CDPC) će u suradnji sa strankama provesti reviziju sviju odredaba Konvencije te će, ako to bude potrebno, preporučiti odgovarajuće izmjene i dopune.

4. Osim kada Vijeće Europe preuzme troškove nastale pri provedbi odredaba stavka 1. ovoga članka, njih će snositi stranke na način koji same utvrde.

5. Tajništvo Vijeća Europe pomagat će strankama pri izvršavanju njihovih funkcija u skladu s ovim člankom.

Članak 47. – OTKAZ

1. Svaka stranka može svakodobno otkazati ovu Konvenciju notifikacijom upućenom Glavnom tajniku Vijeća Europe.

2. Taj će otkaz stupiti na snagu prvoga dana u mjesecu nakon isteka razdoblja od tri mjeseca nakon dana kada je Glavni tajnik primio notifikaciju.

Članak 48. – NOTIFIKACIJA

Glavni tajnik Vijeća Europe će notificirati države članice Vijeća Europe, države nečlanice koje su sudjelovale u izradi ove Konvencije, kao i sve države koje su joj pristupile ili su bile pozvane da joj pristupe o:

a. svim potpisima;

b. polaganju svih isprava o ratifikaciji, prihvatu, odobrenju ili pristupu,

c. svim danima stupanja na snagu ove Konvencije u skladu s člancima 36. i 37.;

d. svim izjavama danim temeljem članaka 40. ili 41. ili rezervama izjavljenima u skladu s

člankom 42.;

e. svim drugim aktima, notifikacijama ili komunikacijama vezanim uz ovu Konvenciju;

U znak prihvata navedenoga, niže potpisani ovlašteni potpisnici potpisuju ovu Konvenciju

U Budimpešti, dne. 23. studenog 2001. godine na engleskom i francuskom jeziku, pri čemu se oba teksta smatraju izvornima, u jednom primjerku koji će biti pohranjen u pismohrani Vijeća Europe. Glavni tajnik Vijeća Europe će ovjerovljene primjerke dostaviti svakoj državi članici Vijeća Europe, državama nečlanicama koje su sudjelovale u izradi ove Konvencije, kao i svim državama pozvanima da joj pristupe.

Članak 3.

Provedba ovoga Zakona u djelokrugu je Ministarstva pravosuđa, uprave i lokalne samouprave, Ministarstva unutarnjih poslova i Ministarstva pomorstva, prometa i veza.

Članak 4.

Na dan stupanja ovoga Zakona na snagu, Konvencija o kibernetičkom kriminalu iz članka 1. ovoga Zakona nije na snazi te će se podaci o njezinom stupanju na snagu objaviti naknadno, u skladu s odredbom članka 30. stavka 3. Zakona o sklapanju i izvršavanju međunarodnih ugovora, nakon njegova stupanja na snagu sukladno odredbi članka 36. Konvencije o kibernetičkom kriminalu.

Članak 5.

Ovaj Zakon stupa na snagu osmoga dana od dana objave u »Narodnim novinama«.

Klasa: 018-05/02-01/08

Zagreb, 3. srpnja 2002.

HRVATSKI SABOR

Predsjednik

Hrvatskoga sabora

Zlatko Tomčić, v. r.