Parte que não nomeou o árbitro que o faça num prazo de dois meses. Se esta Parte não o fizer nesse prazo, o presidente informará desse facto o Secretário Executivo da Comissão Económica para a Europa, que procederá a esta nomeação dentro de um novo prazo de dois meses.

5 — O tribunal arbitral proferirá a sua decisão em conformidade com o direito internacional e com o disposto no presente Protocolo.

6 — Qualquer tribunal arbitral constituído nos termos do disposto no presente anexo estabelecerá o seu próprio regulamento interno.

7 — As decisões do tribunal arbitral relativas quer às questões processuais quer às questões de fundo serão tomadas por maioria dos votos dos seus membros.

8 — O tribunal pode tomar todas as medidas necessárias para apurar os factos.

9 — As Partes no litígio facilitarão o trabalho do tribunal arbitral e, nomeadamente, utilizando todos os meios ao seu dispor:

a) Fornecer-lhe-ão todos os documentos, meios e informações pertinentes;

b) Permitir-lhe-ão, se tal for necessário, citar e ouvir testemunhas ou peritos.

10 — As Partes e os árbitros velarão pela protecção da confidencialidade de todas as informações que receberem a título confidencial no decurso do processo de arbitragem.

11 — O tribunal arbitral pode, a pedido de uma das partes, recomendar a aplicação de medidas cautelares.

12 — Se uma das Partes em litígio não comparecer perante o tribunal arbitral ou não apresentar defesa, a outra Parte pode solicitar ao tribunal que prossiga o processo e profira a sua decisão final. O facto de uma Parte não comparecer ou não apresentar defesa não constitui obstáculo à tramitação do processo. Antes de proferir a sua decisão final, o tribunal arbitral deve certificar-se de que o pedido está bem fundamentado de facto e de direito.

13 — O tribunal arbitral pode apreciar e decidir sobre os pedidos reconvencionais directamente decorrentes do objecto do litígio.

14 — Salvo decisão em contrário do tribunal arbitral justificada pelas circunstâncias particulares do caso, as despesas do tribunal, incluindo os honorários dos árbitros, serão suportadas em partes iguais pelas Partes em litígio. O tribunal manterá um registo de todas as suas despesas e enviará uma relação final das mesmas às Partes.

15 — Qualquer Parte no presente Protocolo que possua um interesse tutelado pela ordem jurídica no objecto do litígio e que possa ser afectada por uma decisão sobre o caso pode intervir no processo, com o acordo do tribunal.

16 — O tribunal arbitral proferirá a sua sentença no prazo de cinco meses a contar da data da sua constituição, a menos que considere necessário prolongar esse prazo por um período que não deverá ser superior a cinco meses.

17 — A sentença do tribunal arbitral será acompanhada de uma declaração apresentando os motivos que a fundamentam. Será definitiva e obrigatória para todas as Partes em litígio. A sentença será comunicada pelo tribunal arbitral às Partes em litígio e ao secretariado. O secretariado enviará as informações recebidas a todas as Partes no presente Protocolo.

18 — Os litígios relativos à interpretação ou à execução da sentença que possam eventualmente surgir entre as Partes serão apresentados por qualquer delas ao tribunal arbitral que proferiu a sentença ou, na impossibilidade de recorrer a esse tribunal, a um outro tribunal constituído para o efeito segundo as mesmas regras que presidiram à constituição do primeiro.

Resolução da Assembleia da República n.º 88/2009

Aprova a Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001

A Assembleia da República resolve, nos termos da alínea *i*) do artigo 161.º e do n.º 5 do artigo 166.º da Constituição, o seguinte:

Artigo 1.º

Aprovação

Aprova a Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001, cujo texto, na versão autenticada na língua inglesa, assim como a respectiva tradução para a língua portuguesa, se publica em anexo.

Artigo 2.º

Reserva

No momento da ratificação da Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001, a República Portuguesa formula a seguinte reserva ao artigo 24.º, n.º 5:

«Portugal não concederá a extradição de pessoas:

a) Que devam ser julgadas por um tribunal de excepção ou cumprir uma pena decretada por um tribunal dessa natureza;

b) Quando se prove que são sujeitas a processo que não oferece garantias jurídicas de um procedimento penal que respeite as condições internacionalmente reconhecidas como indispensáveis à salvaguarda dos direitos do homem, ou que cumprirem a pena em condições desumanas;

c) Quando reclamadas por infracção a que corresponda pena ou medida de segurança com carácter perpétuo.

Portugal só admite a extradição por crime punível com pena privativa da liberdade superior a um ano.

Portugal não concederá a extradição de cidadãos portugueses.

Não há extradição em Portugal por crimes a que corresponda pena de morte segundo a lei do Estado requerente.

Portugal só autoriza o trânsito em território nacional de pessoa que se encontre nas condições em que a sua extradição possa ser concedida.»

Aprovada em 10 de Julho de 2009.

O Presidente da Assembleia da República, *Jaime Gama.*

CONVENTION ON CYBERCRIME

Preamble

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

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

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

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

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

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

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

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

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

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

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

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

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

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

Recalling Committee of Ministers Recommendations no. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, no. R (88) 2 on piracy in the field of copyright and neighbouring rights, no. R (87) 15 regulating the use of personal data in the police sector, no. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as no. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and no. R (95) 13 concerning problems of criminal procedural law connected with information technology;

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

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

have agreed as follows:

CHAPTER I

Use of terms

Article 1

Definitions

For the purposes of this Convention:

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

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

c) «Service provider» means:

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

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

d) «Traffic data» means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

CHAPTER II

Measures to be taken at the national level

SECTION 1

Substantive criminal law

TITLE 1

Offences against the confidentiality, integrity and availability of computer data and systems

Article 2

Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3

Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4

Data interference

1 — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 — A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5

System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6

Misuse of devices

1 — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a) The production, sale, procurement for use, import, distribution or otherwise making available of:

i) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above articles 2 through 5;

ii) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed;

with intent that it be used for the purpose of committing any of the offences established in articles 2 through 5; and

b) the possession of an item referred to in paragraphs *a*), *i*) or *ii*), above, with intent that it be used for the purpose of committing any of the offences established in articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 — This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 — Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1, *a*), *ii*), of this article.

TITLE 2

Computer-related offences

Article 7

Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8

Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and

without right, the causing of a loss of property to another person by:

a) Any input, alteration, deletion or suppression of computer data;
b) Any interference with the functioning of a computer system;

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

TITLE 3

Content-related offences

Article 9

Offences related to child pornography

1 — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a) Producing child pornography for the purpose of its distribution through a computer system;
b) Offering or making available child pornography through a computer system;
c) Distributing or transmitting child pornography through a computer system;
d) Procuring child pornography through a computer system for oneself or for another person;
e) Possessing child pornography in a computer system or on a computer-data storage medium.

2 — For the purpose of paragraph 1 above, the term «child pornography» shall include pornographic material that visually depicts:

a) A minor engaged in sexually explicit conduct;
b) A person appearing to be a minor engaged in sexually explicit conduct;
c) Realistic images representing a minor engaged in sexually explicit conduct.

3 — For the purpose of paragraph 2 above, the term «minor» shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
4 — Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs *d*) and *e*), and 2, sub-paragraphs *b*) and *c*).

TITLE 4

Offences related to infringements of copyright and related rights

Article 10

Offences related to infringements of copyright and related rights

1 — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
2 — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
3 — A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

TITLE 5

Ancillary liability and sanctions

Article 11

Attempt and aiding or abetting

1 — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with articles 2 through 10 of the present Convention with intent that such offence be committed.
2 — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with articles 3 through 5, 7, 8, and 9, 1, *a*) and *c*), of this Convention.
3 — Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12

Corporate liability

1 — Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a) A power of representation of the legal person;
b) An authority to take decisions on behalf of the legal person;
c) An authority to exercise control within the legal person.

2 — In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held

liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 — Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 — Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13

Sanctions and measures

1 — Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 — Each Party shall ensure that legal persons held liable in accordance with article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

SECTION 2

Procedural law

TITLE 1

Common provisions

Article 14

Scope of procedural provisions

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

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

a) The criminal offences established in accordance with articles 2 through 11 of this Convention;

b) Other criminal offences committed by means of a computer system; and

c) The collection of evidence in electronic form of a criminal offence.

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

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

i) Is being operated for the benefit of a closed group of users; and

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

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

Article 15

Conditions and safeguards

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

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

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

TITLE 2

Expedited preservation of stored computer data

Article 16

Expedited preservation of stored computer data

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

2 — Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 — Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep

confidential the undertaking of such procedures for the period of time provided for by its domestic law.

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

Article 17

Expedited preservation and partial disclosure of traffic data

1 — Each Party shall adopt, in respect of traffic data that is to be preserved under article 16, such legislative and other measures as may be necessary to:

a) Ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b) Ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 — The powers and procedures referred to in this article shall be subject to articles 14 and 15.

TITLE 3

Production order

Article 18

Production order

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

a) A person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b) A service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 — The powers and procedures referred to in this article shall be subject to articles 14 and 15.

3 — For the purpose of this article, the term «subscriber information» means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a) The type of communication service used, the technical provisions taken thereto and the period of service;

b) The subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c) Any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

TITLE 4

Search and seizure of stored computer data

Article 19

Search and seizure of stored computer data

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

a) A computer system or part of it and computer data stored therein; and

b) A computer-data storage medium in which computer data may be stored;

in its territory.

2 — Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 — Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

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

b) Make and retain a copy of those computer data;

c) Maintain the integrity of the relevant stored computer data;

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

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

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

TITLE 5

Real-time collection of computer data

Article 20

Real-time collection of traffic data

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

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

b) Compel a service provider, within its existing technical capability:

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

ii) To co-operate and assist the competent authorities in the collection or recording of;

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

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

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

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

Article 21

Interception of content data

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

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

b) Compel a service provider, within its existing technical capability:

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

ii) To co-operate and assist the competent authorities in the collection or recording of;

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

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

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

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

SECTION 3

Jurisdiction

Article 22

Jurisdiction

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

a) In its territory; or

b) On board a ship flying the flag of that Party; or

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

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

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

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

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

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

CHAPTER III

International co-operation

SECTION 1

General principles

TITLE 1

General principles relating to international co-operation

Article 23

General principles relating to international co-operation

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

TITLE 2

Principles relating to extradition

Article 24

Extradition

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

b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or

reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS no.24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

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

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

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

5 — Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 — If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 — *a*) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

TITLE 3

General principles relating to mutual assistance

Article 25

General principles relating to mutual assistance

1 — The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 — Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in articles 27 through 35.

3 — Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 — Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 — Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26

Spontaneous information

1 — A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 — Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

TITLE 4

Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27

Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 — Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 — *a*) Each Party shall designate a central authority or authorities responsible for sending and answering requests

for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b) The central authorities shall communicate directly with each other;

c) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 — Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 — The requested Party may, in addition to the grounds for refusal established in article 25, paragraph 4, refuse assistance if:

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

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

5 — The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 — Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 — The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 — The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 — *a*) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c) Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e) Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28

Confidentiality and limitation on use

1 — When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 — The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a) Kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition; or

b) Not used for investigations or proceedings other than those stated in the request.

3 — If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 — Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

SECTION 2

Specific provisions

TITLE 1

Mutual assistance regarding provisional measures

Article 29

Expedited preservation of stored computer data

1 — A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 — A request for preservation made under paragraph 1 shall specify:

a) The authority seeking the preservation;

b) The offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c) The stored computer data to be preserved and its relationship to the offence;

d) Any available information identifying the custodian of the stored computer data or the location of the computer system;

e) The necessity of the preservation; and

f) That the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 — Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 — A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 — In addition, a request for preservation may only be refused if:

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

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

6 — Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 — Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30

Expedited disclosure of preserved traffic data

1 — Where, in the course of the execution of a request made pursuant to article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

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

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

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

TITLE 2

Mutual assistance regarding investigative powers

Article 31

Mutual assistance regarding accessing of stored computer data

1 — A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to article 29.

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

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

a) There are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b) The instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited cooperation.

Article 32

Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a) Access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b) Access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33

Mutual assistance in the real-time collection of traffic data

1 — The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 — Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34

Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

TITLE 3

24/7 Network

Article 35

24/7 Network

1 — Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) The provision of technical advice;
b) The preservation of data pursuant to articles 29 and 30;
c) The collection of evidence, the provision of legal information, and locating of suspects.

2 — *a*) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.
3 — Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

CHAPTER IV

Final provisions

Article 36

Signature and entry into force

1 — This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.
2 — This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
3 — This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.
4 — In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37

Accession to the Convention

1 — After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in article 20, *d*), of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
2 — In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38

Territorial application

1 — Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
2 — Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.
3 — Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39

Effects of the Convention

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

— The European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS no.24);
— The European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS no. 30);
— The Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS no. 99).

2 — If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein,

they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

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

Article 40

Declarations

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

Article 41

Federal clause

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

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

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

Article 42

Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in article 4, paragraph 2, article 6, paragraph 3, article 9, paragraph 4, article 10, paragraph 3, article 11, paragraph 3, article 14, paragraph 3, article 22, paragraph 2, article 29, paragraph 4, and article 41, paragraph 1. No other reservation may be made.

Article 43

Status and withdrawal of reservations

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

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

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

Article 44

Amendments

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

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

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

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

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

Article 45

Settlement of disputes

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

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

Article 46

Consultations of the Parties

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

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

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

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

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

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

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

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

Article 47

Denunciation

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

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

Article 48

Notification

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

a) Any signature;

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

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

d) Any declaration made under article 40 or reservation made in accordance with article 42;

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

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

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

CONVENÇÃO SOBRE O CIBERCRIME

Preâmbulo

Os Estados membros do Conselho da Europa e os outros Estados signatários:

Considerando que o objectivo do Conselho da Europa é o de criar uma união mais estreita entre os seus membros;

Reconhecendo a importância de intensificar a cooperação com os outros Estados Partes na presente Convenção;

Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objectivo de proteger a sociedade do cibercrime, nomeadamente através da adopção de legislação adequada e do fomento da cooperação internacional;

Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas;

Preocupados com o risco das redes informáticas e da informação electrónica também poderem ser utilizadas para cometer infracções penais e das provas dessas infracções poderem ser armazenadas e transmitidas através dessas redes;

Reconhecendo a necessidade de haver cooperação entre os Estados e a indústria privada no combate ao cibercrime, bem como a de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias de informação;

Acreditando que uma luta efectiva contra o cibercrime requer uma cooperação internacional em matéria penal mais intensa, rápida e eficaz;

Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, prevendo a criminalização desses comportamentos, tal como se encontram descritos na presente Convenção, e a criação de competências suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e a acção penal relativamente às referidas infracções, tanto ao nível nacional como ao nível internacional, e adoptando medidas que visem uma cooperação internacional rápida e fiável;

Tendo presente a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do homem consagrados na Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950), no Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas (1966) e noutros tratados internacionais em matéria de direitos humanos, que reafirmam o direito à liberdade de opinião sem interferência, bem como o direito à liberdade de expressão, incluindo a liberdade de procurar, receber e transmitir, sem consideração de fronteiras, informações e ideias de todo o género e, ainda, o direito ao respeito da vida privada;

Tendo igualmente presente o direito à protecção de dados pessoais, tal como definido na Convenção do Conselho da Europa para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal de 1981;

Considerando a Convenção das Nações Unidas sobre os Direitos da Criança de 1989, e a Convenção da Organização Internacional do Trabalho sobre as Piores Formas de Trabalho Infantil de 1999;

Tendo em conta as Convenções do Conselho da Europa sobre cooperação em matéria penal, bem como outros tratados semelhantes entre os Estados membros do Conselho da Europa e outros Estados, e sublinhando que a presente Convenção tem por finalidade complementar as referidas Convenções de modo a tornar mais eficazes as investigações e as acções penais relativas a infracções relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas electrónicas de uma infracção penal;

Saudando as iniciativas recentes para melhorar o entendimento e a cooperação internacionais no combate ao cibercrime, nomeadamente as acções empreendidas pelas Nações Unidas, pela OCDE, pela União Europeia e pelo G8;

Recordando as Recomendações do Comité de Ministros n.º R (85) 10 relativa à aplicação prática da Convenção Europeia de Auxílio Judiciário Mútuo em matéria penal no tocante às cartas rogatórias para intercepção de telecomunicações, n.º R (88) 2 sobre as medidas destinadas a combater a pirataria no domínio dos direitos de autor e direitos conexos, n.º R (87) 15 que regulamenta a utilização de dados pessoais no sector da polícia, n.º R (95) 4 sobre a protecção de dados de carácter pessoal no sector das telecomunicações, designadamente os serviços telefónicos, e n.º R (89) 9 sobre a criminalidade informática que estabelece directrizes para os legisladores nacionais respeitantes à definição de certos crimes informáticos, e ainda a n.º R (95) 13 relativa a problemas da lei processual penal ligados às tecnologias da informação;

Tendo em conta a Resolução n.º 1 adoptada pelos Ministros europeus da Justiça na sua 21.ª Conferência (Praga, 10 e 11 de Junho de 1997), que recomenda ao Comité de Ministros o apoio ao trabalho desenvolvido pelo Comité Europeu para os Problemas Criminais (CDPC) no domínio do cibercrime, a fim de aproximar as legislações penais nacionais e de permitir a utilização de meios eficazes para investigar esses crimes, bem como a Resolução n.º 3 adoptada na 23.ª Conferência dos Ministros europeus da Justiça (Londres, 8 e 9 de Junho de 2000), que encoraja as partes intervenientes nas negociações a prosseguirem os seus esforços para encontrar soluções adequadas que permitam ao maior número possível de Estados tornarem-se partes da Convenção, e reconhece a necessidade de haver um sistema de cooperação internacional rápido e eficaz que tenha devidamente em conta as exigências específicas da luta contra o cibercrime;

Tendo, igualmente, em consideração o Plano de Acção que foi adoptado pelos Chefes de Estado e de Governo do Conselho da Europa na sua Segunda Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997) para, com base nas normas e nos valores do Conselho da Europa, encontrar respostas comuns face ao desenvolvimento das novas tecnologias de informação;

acordam no seguinte:

CAPÍTULO I

Terminologia

Artigo 1.º

Definições

Para efeitos da presente Convenção, entende-se por:

a) «Sistema informático» um equipamento ou conjunto de equipamentos interligados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o tratamento automatizado de dados;

b) «Dados informáticos» qualquer representação de factos, informações ou conceitos numa forma adequada para o processamento informático, incluindo um programa que permita a um sistema informático executar uma função;

c) «Prestador de serviços»:

i) Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicarem por meio de um sistema informático;

ii) Qualquer outra entidade que processe ou armazene dados informáticos em nome desse serviço de comunicações ou dos seus utilizadores;

d) «Dados de tráfego», quaisquer dados informáticos relativos a uma comunicação efectuada por meio de um sistema informático, que foram gerados por um sistema informático enquanto elemento da cadeia de comunicação, e indicam a origem, o destino, o trajecto, a hora, a data, o tamanho e a duração da comunicação, ou o tipo de serviço subjacente.

CAPÍTULO II

Medidas a adoptar a nível nacional

SECÇÃO 1

Direito penal material

TÍTULO 1

Infracções contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos

Artigo 2.º

Acesso ilícito

Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticado intencionalmente, o acesso ilícito a um sistema informático no seu todo ou a parte dele. Para que se verifique a infracção penal, qualquer uma das Partes pode exigir que ela seja cometida por meio da violação das medidas de segurança com intenção de obter dados informáticos ou com qualquer outra intenção, ou ainda que esteja relacionada com um sistema informático conectado a outro sistema informático.

Artigo 3.º

Intercepção ilícita

Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticada intencionalmente, a intercepção não autorizada, através de meios técnicos, de transmissões não públicas de dados informáticos, para, de ou dentro de um sistema informático, incluindo as radiações electromagnéticas emitidas por um sistema informático que transporte esses dados informáticos. Para que se verifique a infracção penal, qualquer uma das Partes pode exigir que ela seja cometida por meio da violação das medidas de segurança com intenção de obter dados informáticos ou com qualquer outra intenção, ou ainda que esteja relacionada com um sistema informático conectado a outro sistema informático.

Artigo 4.º

Dano provocado nos dados

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno, quando praticados intencionalmente, a danificação, o apagamento, a deterioração, a alteração ou supressão não autorizados de dados informáticos.

2 — Qualquer uma das Partes pode reservar-se o direito de exigir que o comportamento descrito no n.º 1 do presente artigo tenha de ter acarretado danos graves.

Artigo 5.º

Sabotagem informática

Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticada intencionalmente, a perturbação grave, não autorizada, do funcionamento de um sistema informático mediante inserção, transmissão, danificação, eliminação, deterioração, alteração ou supressão de dados informáticos.

Artigo 6.º

Utilização indevida de dispositivos

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno, quando praticadas intencional e ilicitamente:

a) A produção, venda, aquisição para efeitos de utilização, importação, distribuição, ou outras formas de disponibilização de:

i) Um dispositivo, incluindo um programa informático, concebido ou adaptado antes de mais para permitir a prática de uma das infracções previstas nos artigos 2.º a 5.º supra;

ii) Uma palavra passe, um código de acesso ou dados similares que permitem aceder, no todo ou em parte, a um sistema informático, com a intenção de os utilizar;

para cometer qualquer uma das infracções previstas nos artigos 2.º a 5.º supra; e

b) A posse de um dos elementos referidos na alínea *a*), *i*) ou *ii*), desde que utilizados com a intenção de cometer qualquer uma das infracções previstas nos artigos 2.º a 5.º Qualquer uma das Partes pode exigir que para existir responsabilidade criminal nos termos do seu direito interno tenha de se verificar um determinado número desses elementos.

2 — O presente artigo não pode ser interpretado no sentido de determinar que existe responsabilidade criminal nos casos em que a finalidade da produção, venda, obtenção para utilização, importação, distribuição ou outras formas de disponibilização referidas no n.º 1 do presente artigo não é a prática de uma das infracções previstas nos artigos 2.º a 5.º da presente Convenção, mas antes a realização de testes autorizados ou a protecção de um sistema informático.

3 — Cada Parte pode reservar-se o direito de não aplicar o n.º 1 do presente artigo, desde que essa reserva não diga respeito à venda, distribuição ou qualquer outra forma de disponibilização dos elementos referidos no n.º 1, alínea *a*), *ii*), do presente artigo.

TÍTULO 2

Infracções relacionadas com computadores

Artigo 7.º

Falsificação informática

Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno, quando praticadas intencional e ilicitamente, a introdução, a alteração, o apagamento ou a supressão de dados informáticos dos quais resultem dados não autênticos, com o intuito de que esses dados sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Qualquer uma das Partes pode exigir que para existir responsabilidade criminal tem de haver intenção fraudulenta ou outra intenção criminosa semelhante.

Artigo 8.º

Burla informática

Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticado intencional e ilicitamente, o prejuízo patrimonial causado a outra pessoa por meio de:

a) Qualquer introdução, alteração, apagamento ou supressão de dados informáticos;

b) Qualquer interferência no funcionamento de um sistema informático;

com intenção de obter para si ou para outra pessoa um benefício económico ilegítimo.

TÍTULO 3

Infracções relacionadas com o conteúdo

Artigo 9.º

Infracções relativas à pornografia infantil

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno, quando praticadas de forma intencional e ilegítima, as seguintes condutas:

a) Produção de pornografia infantil com o propósito de a divulgar através um sistema informático;

b) Oferta ou disponibilização de pornografia infantil através de um sistema informático;

c) Difusão ou transmissão de pornografia infantil através de um sistema informático;

d) Obtenção para si ou para outra pessoa de pornografia infantil através de um sistema informático;

e) Posse de pornografia infantil num sistema informático ou num dispositivo de armazenamento de dados informáticos.

2 — Para efeitos do n.º 1, a expressão «pornografia infantil» deverá abranger todo o material pornográfico que represente visualmente:

a) Um menor envolvido em comportamentos sexualmente explícitos;
b) Uma pessoa com aspecto de menor envolvida em comportamentos sexualmente explícitos;
c) Imagens realistas de um menor envolvido em comportamentos sexualmente explícitos.

3 — Para efeitos do n.º 2, a expressão «menor» deverá abranger qualquer pessoa com menos de 18 anos de idade. Qualquer uma das Partes pode impor um limite de idade inferior, não podendo, contudo, ser fixado abaixo dos 16 anos.
4 — Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nas alíneas *d*) e *e*) do n.º 1 e nas alíneas *b*) e *c*) do n.º 2.

TÍTULO 4

Infracções respeitantes a violações do direito de autor e direitos conexos

Artigo 10.º

Infracções respeitantes a violações do direito de autor e dos direitos conexos

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno, as violações do direito de autor, tal como estas se encontram definidas na lei dessa Parte com base nas obrigações que a mesma assumiu ao abrigo da Convenção de Berna para a Protecção das Obras Literárias e Artísticas, revista pelo Acto de Paris de 24 de Julho de 1971, do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio e do Tratado da OMPI sobre o Direito de Autor, com excepção de quaisquer direitos morais reconhecidos por essas Convenções, quando tais actos são praticados de forma intencional, para fins comerciais e por meio de um sistema informático.
2 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais nos termos do seu direito interno as violações dos direitos conexos tal como estas se encontram definidas na lei dessa Parte com base nas obrigações que a mesma assumiu ao abrigo da Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão (Convenção de Roma), do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio e do Tratado da OMPI sobre Interpretações ou Execuções e Fonogramas, com excepção de quaisquer direitos morais reconhecidos por essas Convenções, quando tais actos são praticados de forma intencional, para fins comerciais e por meio de um sistema informático.
3 — Qualquer Parte pode, em circunstâncias claramente definidas, reservar-se o direito de não estabelecer a responsabilidade criminal nos termos dos n.os 1 e 2 do presente artigo, desde que se encontrem disponíveis outros meios eficazes e essa reserva não prejudique as obrigações internacionais assumidas por essa Parte no quadro dos instrumentos internacionais referidos nos n.os 1 e 2 do presente artigo.

TÍTULO 5

Outras formas de responsabilidade e sanções

Artigo 11.º

Tentativa, auxílio ou instigação

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracções penais, nos termos do seu direito interno, o auxílio ou a instigação à prática de qualquer uma das infracções previstas nos artigos 2.º a 10.º da presente Convenção, quando praticados intencionalmente tendo em vista a prática dessa infracção.
2 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal, nos termos do seu direito interno, a tentativa deliberada de praticar qualquer uma das infracções previstas nos artigos 3.º a 5.º , 7.º, 8.º e nas alíneas *a*) e *c*) do n.º 1 do artigo 9.º da presente Convenção.
3 — Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.º 2 do presente artigo.

Artigo 12.º

Responsabilidade das pessoas colectivas

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para garantir que as pessoas colectivas possam ser consideradas responsáveis pelas infracções penais previstas na presente Convenção, cometidas em seu benefício por qualquer pessoa singular, agindo individualmente ou enquanto membro de um órgão da pessoa colectiva, que nelas ocupem uma posição de liderança, com base:

a) Nos poderes de representação conferidos pela pessoa colectiva;
b) Na autoridade para tomar decisões em nome da pessoa colectiva;
c) Na autoridade para exercer o controlo no seio da pessoa colectiva.

2 — Para além dos casos já previstos no n.º 1 do presente artigo, cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para garantir que uma pessoa colectiva possa ser considerada responsável sempre que a falta de vigilância ou controlo por parte de uma pessoa singular referida no n.º 1 possibilite a prática de uma das infracções previstas na presente Convenção em benefício da referida pessoa colectiva por uma pessoa singular que aja sob a sua autoridade.
3 — De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser penal, civil ou administrativa.
4 — Essa responsabilidade não exclui a responsabilidade criminal das pessoas singulares que tenham cometido a infracção.

Artigo 13.º

Sanções e medidas

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para assegurar que as infracções penais estabelecidas nos termos dos artigos 2.º a 11.º sejam puníveis com sanções eficazes, proporcionais e dissuasivas, incluindo com penas privativas de liberdade.
2 — Cada Parte deverá assegurar que as pessoas colectivas consideradas responsáveis nos termos do artigo 12.º

sejam objecto de sanções ou medidas, de natureza penal e não penal, eficazes, proporcionais e dissuasivas, incluindo sanções pecuniárias.

SECÇÃO 2

Direito processual

TÍTULO 1

Disposições comuns

Artigo 14.º

Âmbito de aplicação das disposições processuais

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para instituir os poderes e os procedimentos previstos na presente secção, para efeitos de investigação ou de procedimento criminal específicos.

2 — Salvo disposição em contrário do artigo 21.º, cada Parte deverá aplicar os poderes e os procedimentos previstos no n.º 1 do presente artigo:

a) Às infracções penais previstas nos artigos 2.º a 11.º da presente Convenção;

b) A outras infracções penais cometidas por meio de um sistema informático; e

c) À obtenção de prova electrónica da prática de qualquer infracção penal.

3 — *a*) Cada Parte pode reservar-se o direito de só aplicar as medidas previstas no artigo 20.º às infracções ou categorias de infracções especificadas na reserva, desde que o conjunto dessas infracções ou categorias de infracções não seja mais reduzido que o conjunto de infracções a que aplica as medidas previstas no artigo 21.º Cada Parte deverá considerar a possibilidade de restringir a dita reserva de modo a permitir que a aplicação da medida prevista no artigo 20.º seja a mais ampla possível.

b) Sempre que por força das restrições impostas pela sua legislação vigente à data da adopção da presente Convenção não possa aplicar as medidas previstas nos artigos 20.º e 21.º às comunicações que se processam no interior de um sistema informático de um prestador de serviços, que:

i) Tenha sido implementado para um grupo fechado de utilizadores; e

ii) Nem utilize as redes de telecomunicações públicas nem esteja interligado a outro sistema informático, público ou privado;

uma Parte pode reservar-se o direito de não aplicar essas medidas às referidas comunicações. Cada Parte deverá considerar a possibilidade de restringir a dita reserva de modo a permitir a aplicação das medidas previstas nos artigos 20.º e 21.º

Artigo 15.º

Condições e garantias

1 — Cada Parte deverá assegurar que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos na presente secção respeitem as condições e garantias previstas no seu direito interno, o qual deverá garantir uma protecção adequada dos direitos humanos e das liberdades, designadamente dos direitos estabelecidos em conformidade com as obrigações assumidas pela Parte em virtude da Convenção do Conselho da Europa de 1950 para a Protecção dos Direitos do Homem e das Liberdades Fundamentais e do Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966, bem como de outros instrumentos internacionais aplicáveis em matéria de direitos humanos, e deverá incorporar o princípio da proporcionalidade.

2 — Sempre que tal se justifique, em razão da natureza do poder ou do procedimento em causa, as referidas condições e garantias deverão incluir, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a delimitação do âmbito de aplicação e a duração do poder ou procedimento em causa.

3 — Na medida em que seja do interesse público, em particular, da boa administração da justiça, cada Parte deverá ter em consideração o impacto dos poderes e dos procedimentos previstos na presente secção nos direitos, nas responsabilidades e nos interesses legítimos de terceiros.

TÍTULO 2

Conservação expedita de dados informáticos armazenados

Artigo 16.º

Conservação expedita de dados informáticos armazenados

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para que as suas autoridades competentes possam ordenar ou de outro modo impor a conservação expedita de dados informáticos específicos, incluindo de dados de tráfego armazenados por meio de um sistema informático, sobretudo quando existam motivos para crer que em relação a esses dados existe o sério risco de perda ou alteração.

2 — Sempre que aplicar o disposto no n.º 1 supra através de uma injunção que impõe a uma pessoa a conservação dos dados informáticos específicos armazenados que tem na sua posse ou sob o seu controlo, uma Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para obrigar essa pessoa a conservar e a proteger a integridade dos referidos dados pelo tempo que for necessário, até um prazo máximo de 90 dias, para permitir que as autoridades competentes obtenham a sua divulgação. Qualquer uma das Partes pode prever a possibilidade dessa injunção ser subsequentemente renovada.

3 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para obrigar a pessoa responsável pelos dados informáticos, ou qualquer outra pessoa encarregue de os conservar, a manterem a confidencialidade da aplicação dos referidos procedimentos durante o prazo previsto no seu direito interno.

4 — Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.

Artigo 17.º

Conservação expedita e divulgação parcial de dados de tráfego

1 — Em relação aos dados de tráfego que devem ser conservados em conformidade com o artigo 16.º, cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para:

a) Assegurar a conservação expedita dos dados de tráfego quer tenha sido um, quer tenham sido vários os

prestadores de serviço envolvidos na transmissão dessa comunicação;

b) Assegurar que um volume suficiente de dados de tráfego seja de imediato transmitido à autoridade competente da Parte ou a qualquer pessoa designada por essa autoridade, para permitir que a Parte identifique os prestadores de serviços e o trajecto da comunicação.

2 — Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.

TÍTULO 3

Injunção de comunicar

Artigo 18.º

Injunção de comunicar

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para conferir poder às suas autoridades competentes para ordenarem:

a) A uma pessoa que se encontre no seu território que disponibilize os dados informáticos específicos que estejam na sua posse ou sob o seu controlo e que estão armazenados num sistema informático ou num dispositivo de armazenamento de dados informáticos; e

b) A um prestador de serviços que preste os seus serviços no território da Parte que disponibilize os dados dos assinantes relacionados com esses serviços que estejam na sua posse ou sob o seu controlo.

2 — Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.

3 — Para efeitos do presente artigo, entende-se por «dados relativos aos assinantes» quaisquer informações que um prestador de serviços possua sobre os assinantes dos seus serviços, sob a forma de dados informáticos ou sob qualquer outra forma, distintas dos dados de tráfego ou de conteúdo e que permitam determinar:

a) O tipo de serviço de comunicação utilizado, as medidas técnicas adoptadas a esse respeito e a duração do serviço;

b) A identidade, o endereço postal ou geográfico e o número de telefone do assinante e qualquer outro número de acesso, os dados referentes à facturação e ao pagamento, disponíveis com base num contrato ou num acordo de serviços;

c) Qualquer outra informação sobre a localização do equipamento de comunicação disponível com base num contrato ou num acordo de prestação de serviços.

TÍTULO 4

Busca e apreensão de dados informáticos armazenados

Artigo 19.º

Busca e apreensão de dados informáticos armazenados

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a efectuar buscas ou de outro modo aceder:

a) A um sistema informático, ou a parte do mesmo, bem como aos dados informáticos nele armazenados; e

b) A um suporte informático de dados que permita armazenar dados informáticos;

no seu território.

2 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para assegurar que, sempre que as suas autoridades efectuem buscas ou de outro modo acedam a um determinado sistema informático ou a parte dele, em conformidade com o disposto na alínea *a*) do n.º 1 do presente artigo, e caso existam motivos para crer que os dados procurados estão armazenados noutro sistema informático ou em parte dele, situado no seu território, e que é possível aceder legalmente a esses dados ou que eles estão disponíveis através do primeiro sistema, as autoridades são capazes de rapidamente alargar a busca ou o acesso equivalente ao outro sistema.

3 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a apreender ou de outro modo reter os dados informáticos aos quais se teve acesso nos termos do n.º 1 ou 2 do presente artigo. Essas medidas incluem o poder de:

a) Apreender ou de outro modo reter um sistema informático ou parte do mesmo, ou um suporte informático de dados;

b) Efectuar e reter uma cópia desses dados informáticos;

c) Preservar a integridade dos dados informáticos pertinentes armazenados;

d) Tornar esses dados informáticos inacessíveis ou retirá-los do sistema informático acedido.

4 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a impor a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas aplicadas para proteger os dados informáticos nele contidos, que forneça de forma ponderada todas as informações necessárias para permitir a aplicação das medidas previstas no n.º 1 e 2 do presente artigo.

5 — Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.

TÍTULO 5

Recolha, em tempo real, de dados informáticos

Artigo 20.º

Recolha, em tempo real, de dados de tráfego

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a:

a) Recolher ou registar, através da aplicação dos meios técnicos existentes no seu território; e

b) Obrigar um prestador de serviços, no âmbito da sua capacidade técnica, a:

i) Recolher ou registar, através da aplicação dos meios técnicos existentes no seu território; ou

ii) Cooperar com as autoridades competentes e a dar-lhes assistência na recolha ou no registo;

em tempo real, dos dados de tráfego associados a comunicações específicas transmitidas no seu território através de um sistema informático.

2 — Quando uma Parte, por força dos princípios estabelecidos no seu direito interno, não puder adoptar as medidas enunciadas na alínea *a*) do n.º 1 do presente artigo, pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias para assegurar a recolha ou o registo, em tempo real, dos dados de tráfego associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.

3 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para obrigar um prestador de serviços a manter a confidencialidade do exercício de um dos poderes previstos no presente artigo, bem como de qualquer informação a esse respeito.

4 — Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.

Artigo 21.º

Intercepção de dados de conteúdo

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes, relativamente a um conjunto de infracções graves a definir no âmbito do seu direito interno, a:

a) Recolher ou registar, através da aplicação dos meios técnicos existentes no seu território;

b) Obrigar um prestador de serviços, no âmbito da sua capacidade técnica, a:

i) Recolher ou registar, através da aplicação dos meios técnicos existentes no seu território; ou a

ii) Cooperar com as autoridades competentes e a dar-lhes assistência na recolha ou no registo;

em tempo real, dos dados de conteúdo de comunicações específicas feitas no seu território, transmitidas através de um sistema informático.

2 — Quando uma Parte, por força dos princípios estabelecidos no seu direito interno, não puder adoptar as medidas enunciadas na alínea *a*) do n.º 1 do presente artigo, pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias para assegurar a recolha ou o registo, em tempo real, dos dados de conteúdo de comunicações específicas feitas no seu território, transmitidas através de um sistema informático nesse território.

3 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para obrigar um prestador de serviços a manter a confidencialidade do exercício de um dos poderes previstos no presente artigo, bem como de qualquer informação a esse respeito.

4 — Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.

SECÇÃO 3

Jurisdição

Artigo 22.º

Jurisdição

1 — Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente à prática de qualquer infracção penal prevista nos artigos 2.º a 11.º da presente Convenção, sempre que a infracção seja cometida:

a) No seu território; ou

b) A bordo de um navio arvorando o pavilhão dessa Parte;

c) A bordo de uma aeronave registada nos termos das leis dessa Parte;

d) Por um dos seus nacionais, se a infracção for punível nos termos do direito penal vigente no local onde foi praticada, ou se for cometida em local que não se encontra sob a jurisdição territorial de qualquer Estado.

2 — Cada Parte pode reservar-se o direito de não aplicar, ou de apenas aplicar em casos e condições específicas, as regras de competência jurisdicional definidas nas alíneas *b*) a *d*) do n.º 1 do presente artigo ou qualquer parte dessas alíneas.

3 — Cada Parte deverá adoptar as medidas legislativas que se revelem necessárias para estabelecer a sua jurisdição sobre as infracções referidas no n.º 1 do artigo 24.º da presente Convenção, sempre que o presumível autor da infracção se encontre no seu território e não seja extraditado para outra Parte apenas com base na sua nacionalidade, após um pedido de extradição.

4 — A presente Convenção não exclui nenhuma jurisdição penal exercida por uma Parte em conformidade com o seu direito interno.

5 — Sempre que várias Partes reivindiquem a jurisdição sobre uma presumível infracção prevista na presente Convenção, as Partes interessadas deverão, se for caso disso, consultar-se para decidir qual é a jurisdição mais adequada para efeitos de exercício da acção penal.

CAPÍTULO III

Cooperação internacional

SECÇÃO 1

Princípios gerais

TÍTULO 1

Princípios gerais relativos à cooperação internacional

Artigo 23.º

Princípios gerais relativos à cooperação internacional

As Partes deverão cooperar o mais possível entre si para efeitos de investigação ou de procedimento relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para recolha de provas sob a forma electrónica de uma infracção penal, em conformidade com o disposto no presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre cooperação internacional em matéria penal, de acordos celebrados com base em legislação uniforme ou recíproca e dos respectivos Direitos internos.

TÍTULO 2

Princípios relativos à extradição

Artigo 24.º

Extradição

1 — *a*) O presente artigo aplica-se à extradição entre as Partes para as infracções penais previstas nos artigos 2.º

a 11.º da presente Convenção, desde que sejam puníveis, nos termos da legislação das duas Partes interessadas, com uma pena privativa de liberdade de duração máxima não inferior a um ano ou com uma pena mais grave.

b) Nos casos em que seja aplicável uma pena mínima diferente, nos termos de um acordo celebrado com base em legislação uniforme ou recíproca ou de um tratado de extradição aplicável entre duas ou mais Partes, incluindo a Convenção Europeia de Extradição (STE n.º 24), dever-se-á aplicar a pena mínima prevista nesse tratado ou acordo.

2 — As infracções penais descritas no n.º 1 do presente artigo deverão ser consideradas como estando incluídas em qualquer tratado de extradição existente entre as Partes como infracções passíveis de extradição. As Partes comprometem-se a incluir essas infracções em qualquer tratado de extradição que venha a ser celebrado entre elas como infracções passíveis de extradição.

3 — Sempre que uma Parte receber um pedido de extradição proveniente de outra Parte com a qual não celebrou nenhum tratado de extradição e fizer depender a extradição da existência de um tratado, pode considerar a presente Convenção como constituindo a base legal para a extradição relativamente às infracções penais previstas no n.º 1 do presente artigo.

4 — As Partes que não façam depender a extradição da existência de um tratado deverão reconhecer entre si as infracções penais referidas no n.º 1 do presente artigo como infracções passíveis de extradição.

5 — A extradição fica sujeita às condições previstas na lei da Parte requerida ou nos tratados de extradição aplicáveis, incluindo os motivos pelos quais a Parte requerida pode recusar a extradição.

6 — Se a extradição por uma das infracções penais previstas no n.º 1 do presente artigo for recusada apenas com base na nacionalidade da pessoa procurada ou porque a Parte requerida considera ter competência relativamente a essa infracção, a Parte requerida deverá, a pedido da Parte requerente, apresentar o caso às suas autoridades competentes para fins de procedimento criminal e informar oportunamente a Parte requerente do resultado definitivo. Essas autoridades deverão tomar a sua decisão e conduzir as investigações e o procedimento nas mesmas condições que para qualquer outra infracção de natureza idêntica, nos termos da lei dessa Parte.

7 — *a*) Na falta de tratado, cada Parte deverá, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, comunicar ao Secretário-Geral do Conselho da Europa o nome e a morada de cada autoridade responsável pela elaboração ou recepção dos pedidos de extradição ou de detenção provisória.

b) O Secretário-Geral do Conselho da Europa deverá criar e manter actualizado um registo das autoridades assim designadas pelas Partes. Cada Parte deverá assegurar que os dados constantes do registo estão sempre correctos.

TÍTULO 3

Princípios gerais relativos ao auxílio judiciário mútuo

Artigo 25.º

Princípios gerais relativos ao auxílio judiciário mútuo

1 — As Partes deverão conceder-se mutuamente o mais amplo auxílio possível para efeitos de investigação ou de procedimento relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma electrónica de uma infracção penal.

2 — Cada Parte deverá adoptar, igualmente, as medidas legislativas e outras que se revelem necessárias para cumprir as obrigações enunciadas nos artigos 27.º a 35.º

3 — Em caso de urgência, cada Parte pode efectuar os pedidos de auxílio judiciário mútuo ou as comunicações conexas, através de meios de comunicação expeditos, nomeadamente por fax ou correio electrónico, desde que esses meios assegurem níveis de segurança e autenticação adequados (incluindo a encriptação, se necessário), com confirmação oficial posterior se o Estado requerido o exigir. O Estado requerido deverá aceitar e responder ao pedido através de qualquer um desses meios de comunicação expeditos.

4 — Salvo disposição expressa em contrário prevista nos artigos do presente capítulo, o auxílio judiciário mútuo fica sujeito às condições previstas na lei da Parte requerida ou nos tratados de auxílio mútuo aplicáveis, incluindo os motivos pelos quais a Parte requerida pode recusar a cooperação. A Parte requerida não deverá exercer o seu direito de recusa de auxílio judiciário mútuo relativamente às infracções previstas nos artigos 2.º a 11.º apenas com o fundamento de que o pedido se reporta a uma infracção considerada como uma infracção de natureza fiscal.

5 — Sempre que, em conformidade com o disposto no presente capítulo, a Parte requerida estiver autorizada a fazer depender o auxílio judiciário mútuo da existência de dupla incriminação, considera-se que esta condição está preenchida se a conduta que constitui a infracção, relativamente à qual o auxílio mútuo é pedido, for qualificada como infracção penal pelo direito interno dessa Parte, independentemente de nos termos do seu direito interno a infracção pertencer ou não à mesma categoria de infracções ou obedecer ou não à mesma terminologia que as previstas no direito interno da Parte requerente.

Artigo 26.º

Informação espontânea

1 — Qualquer Parte pode, nos limites previstos no seu direito interno e não e sem pedido prévio, transmitir a uma outra Parte informações obtidas no âmbito das suas próprias investigações, sempre que considerar que a transmissão dessas informações pode ajudar a Parte destinatária a iniciar ou a efectuar investigações ou procedimentos relativos a infracções penais previstas na presente Convenção, ou sempre que considerar que ela pode dar origem a um pedido de cooperação formulado por essa Parte nos termos do presente capítulo.

2 — Antes de transmitir essas informações, a Parte transmissora pode solicitar que o seu carácter confidencial seja preservado ou que só sejam utilizadas em determinadas condições. Se não puder satisfazer o pedido, a Parte destinatária deverá informar a outra Parte de tal facto, a qual deverá, então, decidir se as informações em causa devem, mesmo assim, ser fornecidas. Se a Parte destinatária aceitar as informações nas condições estipuladas, fica obrigada a observá-las.

TÍTULO 4

Procedimentos relativos a pedidos de auxílio mútuo na falta de acordos internacionais aplicáveis

Artigo 27.º

Procedimentos relativos aos pedidos de auxílio mútuo na falta de acordos internacionais aplicáveis

1 — Na falta de um tratado de auxílio mútuo ou de um acordo assente em legislação uniforme ou recíproca em vigor entre a Parte requerente e a Parte requerida, aplica-se o disposto nos n.os 2 a 9 do presente artigo. Existindo esse tratado, acordo ou legislação, só se aplica o disposto no presente artigo se, em vez deles, as Partes envolvidas decidirem aplicar o presente artigo, no todo ou em parte.

2 — *a*) Cada Parte deverá designar uma ou mais autoridades centrais encarregues de enviar os pedidos de auxílio mútuo ou de lhes responder, de os executar ou de os transmitir às autoridades competentes com vista à sua execução;

b) As autoridades centrais deverão comunicar directamente entre si;

c) Cada Parte deverá, no momento em que assinar ou depositar o seu instrumento de ratificação, aceitação, aprovação ou adesão, comunicar ao Secretário-Geral do Conselho da Europa o nome e endereço das autoridades designadas nos termos do presente número;

d) O Secretário-Geral do Conselho da Europa deverá criar e manter actualizado um registo das autoridades centrais designadas pelas Partes. Cada Parte deverá assegurar que os dados constantes do registo estão sempre correctos.

3 — Os pedidos de auxílio mútuo referidos no presente artigo deverão ser executados em conformidade com os procedimentos especificados pela Parte requerente, salvo se forem incompatíveis com a legislação da Parte requerida.

4 — Para além dos motivos de recusa previstos no n.º 4 do artigo 25.º, a Parte requerida pode recusar o auxílio mútuo se considerar que:

a) O pedido respeita a uma infracção de natureza política ou com ela conexa; ou que

b) A execução do pedido pode prejudicar a sua soberania, segurança, ordem pública ou outros interesses essenciais.

5 — A Parte requerida pode adiar a execução do pedido sempre que ela prejudique as investigações ou os procedimentos criminais levados a cabo pelas suas autoridades.

6 — Antes de recusar ou adiar o auxílio, a Parte requerida deverá, se for caso disso, após consulta com a Parte requerente, verificar se o pedido pode ser parcialmente executado ou sujeito às condições que considere necessárias.

7 — A Parte requerida deverá de imediato informar a Parte requerente do resultado da execução do pedido de auxílio. Qualquer recusa ou adiamento do pedido deverão ser fundamentados. A Parte requerida também deverá informar a Parte requerente de quaisquer motivos que impossibilitem a execução do pedido ou que conduzam a um atraso significativo da mesma.

8 — A Parte requerente pode solicitar à Parte requerida que preserve a confidencialidade de qualquer pedido apresentado nos termos do presente capítulo bem como do respectivo conteúdo, a menos que a sua execução exija o contrário. Caso não possa respeitar o pedido de confidencialidade, a Parte requerida deverá de imediato informar a Parte requerente, a qual decide depois se o pedido deve, ainda assim, ser executado.

9 — *a*) Nos casos urgentes, as autoridades judiciárias da Parte requerente podem enviar directamente às autoridades judiciárias da Parte requerida os pedidos de auxílio mútuo ou as comunicações com eles relacionadas. Nesses casos, dever-se-á ao mesmo tempo e por intermédio da autoridade central da Parte requerente enviar uma cópia à autoridade central da Parte requerida.

b) Qualquer pedido ou comunicação nos termos do presente número podem ser efectuados por intermédio da Organização Internacional de Polícia Criminal (Interpol).

c) Quando um pedido é efectuado nos termos da alínea *a*) do presente artigo e a autoridade não é competente para executá-lo, deverá esta última transmiti-lo à autoridade nacional competente e informar directamente a Parte requerente de tal facto.

d) As autoridades competentes da Parte requerente podem enviar directamente às autoridades competentes da Parte requerida os pedidos ou as comunicações nos termos do presente número que não envolvam medidas coercivas.

e) Cada Parte pode, no momento em que assinar ou depositar o seu instrumento de ratificação, aceitação, aprovação ou adesão, informar o Secretário-Geral do Conselho da Europa que, por razões de eficácia, os pedidos feitos nos termos do presente número deverão ser dirigidos à sua autoridade central.

Artigo 28.º

Confidencialidade e restrição de utilização

1 — Na falta de um tratado de auxílio mútuo ou de um acordo assente em legislação uniforme ou recíproca em vigor entre a Parte requerente e a Parte requerida, aplica-se o disposto no presente artigo. Existindo esse tratado, acordo ou legislação, só se aplica o disposto no presente artigo se, em vez deles, as Partes envolvidas decidirem aplicar o presente artigo, no todo ou em parte.

2 — A Parte requerida pode sujeitar a comunicação de informações ou de material em resposta a um pedido às seguintes condições:

a) É mantida a confidencialidade dessas informações e desse material nos casos em que o pedido de auxílio mútuo não puder ser cumprido sem o preenchimento dessa condição, ou

b) Essas informações e esse material não são utilizados para investigações ou procedimentos diversos dos indicados no pedido.

3 — Se não puder satisfazer uma das condições enunciadas no n.º 2 do presente artigo, a Parte requerente deverá de imediato informar a Parte requerida, a qual decide depois se a informação deve, ainda assim, ser transmitida. Se aceitar essa condição, a Parte requerente fica obrigada a observá-la.

4 — Qualquer Parte que forneça informações ou material sujeitos a uma das condições enunciadas no n.º 2 do presente artigo pode exigir da outra Parte uma explicação sobre a utilização dada a essas informações ou a esse material.

SECÇÃO 2

Disposições específicas

TÍTULO 1

Auxílio mútuo em matéria de medidas cautelares

Artigo 29.º

Conservação expedita de dados informáticos armazenados

1 — Uma Parte pode solicitar a outra Parte que ordene ou, de outro modo, imponha a conservação expedita de dados armazenados através de um sistema informático situado no território dessa outra Parte, e relativamente aos quais a Parte requerente pretende efectuar um pedido de auxílio mútuo tendo em vista a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, ou a divulgação dos dados.

2 — Um pedido de conservação feito nos termos do n.º 1 do presente artigo deverá especificar:

a) A autoridade que solicita a conservação;

b) A infracção que constitui o objecto da investigação ou do procedimento criminal, bem como um breve resumo dos respectivos factos;

c) Os dados informáticos armazenados que devem ser conservados e a relação entre estes e a infracção;

d) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos armazenados ou a localização do sistema informático;

e) A necessidade da conservação; e

f) A intenção da Parte de apresentar um pedido de auxílio tendo em vista a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, ou a divulgação de dados informáticos armazenados.

3 — Após ter recebido o pedido de outra Parte, a Parte requerida deverá tomar todas as medidas adequadas para proceder, de forma expedita, à conservação dos dados especificados, em conformidade com o seu direito interno. Para efeitos de execução de um pedido, o requisito da dupla incriminação não é exigido como condição para essa conservação.

4 — Uma Parte que imponha o requisito da dupla incriminação como condição para executar um pedido de auxílio mútuo tendo em vista a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, ou a divulgação dos dados, pode, em relação a outras infracções que não as estabelecidas em conformidade com o disposto nos artigos 2.º a 11.º da presente Convenção, reservar-se o direito de recusar o pedido de conservação nos termos do presente artigo nos casos em que tenha motivos para crer que, no momento da divulgação, o requisito da dupla incriminação não pode ser preenchido.

5 — Além disso, um pedido de conservação só pode ser recusado se a Parte requerida considerar que:

a) O pedido respeita a uma infracção de natureza política ou com ela conexa; ou que

b) A execução do pedido pode prejudicar a sua soberania, segurança, ordem pública ou outros interesses essenciais.

6 — Quando, no seu entender, a conservação não assegurar a futura disponibilização dos dados ou comprometer ou de outro modo prejudicar a confidencialidade das investigações efectuadas pela Parte requerente, a Parte requerida deverá de imediato informar a Parte requerente, a qual decide depois se o pedido deve, ainda assim, ser executado.

7 — Qualquer conservação efectuada em resposta ao pedido referido no n.º 1 do presente artigo é válida por um período não inferior a 60 dias, de modo a permitir que a Parte requerente possa apresentar um pedido tendo em vista a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, ou a divulgação dos dados. Após a recepção desse pedido, os dados deverão continuar a ser conservados até que haja uma decisão sobre o pedido.

Artigo 30.º

Divulgação expedita de dados de tráfego conservados

1 — Quando, no decurso da execução de um pedido de conservação de dados de tráfego relativos a uma determinada comunicação, formulado nos termos do artigo 29.º, verificar que um prestador de serviços noutro Estado participou na transmissão da comunicação, a Parte requerida deverá transmitir rapidamente à Parte requerente dados de tráfego suficientes para identificar esse prestador de serviços bem como o trajecto utilizado para a transmissão da comunicação.

2 — A divulgação de dados de tráfego nos termos do n.º 1 só pode ser recusada se a Parte requerida considerar que:

i) O pedido respeita a uma infracção de natureza política ou com ela conexa; ou que

ii) A execução do pedido pode prejudicar a sua soberania, segurança, ordem pública ou outros interesses essenciais.

TÍTULO 2

Auxílio mútuo no tocante aos poderes de investigação

Artigo 31.º

Auxílio mútuo para o acesso a dados informáticos armazenados

1 — Uma Parte pode solicitar a outra Parte a busca ou outro acesso semelhante, a apreensão ou outro tipo de retenção semelhante, bem como a divulgação de dados armazenados através de um sistema informático situado no território dessa outra Parte, incluindo os dados conservados em conformidade com o artigo 29.º

2 — A Parte requerida deverá cumprir o pedido aplicando os instrumentos internacionais, os acordos e a legislação referidos no artigo 23.º e respeitando as disposições pertinentes do presente capítulo.

3 — O pedido deverá ser cumprido o mais rapidamente possível sempre que:

a) Haja motivos para crer que os dados relevantes são especialmente susceptíveis de se perderem ou de serem alterados;

b) Os instrumentos, os acordos e a legislação referidos no n.º 2 prevejam uma cooperação célere.

Artigo 32.º

Acesso transfronteiriço a dados armazenados num computador, mediante consentimento ou quando se trate de dados acessíveis ao público

Uma Parte pode, sem autorização de uma outra Parte:

a) Aceder a dados informáticos acessíveis ao público (fonte aberta), independentemente da sua localização geográfica;

b) Através de um sistema informático situado no seu território, aceder a dados informáticos no território de uma outra Parte, ou recebê-los, se obtiver o consentimento legal e voluntário da pessoa com legitimidade para lhe divulgar os dados através desse sistema informático.

Artigo 33.º

Auxílio mútuo para a recolha, em tempo real, de dados de tráfego

1 — As Partes deverão conceder-se mutuamente auxílio para a recolha, em tempo real, de dados de tráfego relativos a comunicações específicas transmitidas no seu território por meio de um sistema informático. Sem prejuízo do disposto no n.º 2, o auxílio deverá ser concedido nas condições e de acordo com os procedimentos previstos no direito interno.

2 — Cada Parte deverá conceder esse auxílio pelo menos em relação às infracções penais relativamente às quais, em casos internos semelhantes, seria possível efectuar a recolha, em tempo real, de dados de tráfego.

Artigo 34.º

Auxílio mútuo para a intercepção de dados de conteúdo

As Partes deverão conceder-se mutuamente auxílio para a recolha ou o registo, em tempo real, de dados relacionados com o conteúdo de comunicações específicas transmitidas através de um sistema informático, na medida em que os seus tratados e respectivo direito interno em vigor o permitam.

TÍTULO 3

Rede 24/7

Artigo 35.º

Rede 24/7

1 — Cada Parte deverá designar um ponto de contacto que deverá estar disponível vinte e quatro horas por dia, sete dias por semana, a fim de assegurar de imediato a prestação de auxílio nas investigações e nos procedimentos relativos a infracções penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma electrónica, da prática de infracções penais. Esse auxílio deverá compreender a facilitação ou, se o direito e a prática internos o permitirem, a execução directa das seguintes medidas:

a) O aconselhamento técnico;
b) A conservação de dados em conformidade com os artigos 29.º e 30.º;
c) A recolha de provas, prestação de informações de natureza jurídica e localização de suspeitos.

2 — *a*) O ponto de contacto de uma Parte deverá dispor de meios para contactar com rapidez o ponto de contacto de uma outra Parte.

b) O ponto de contacto designado por uma Parte deverá assegurar que se pode coordenar de forma célere com a ou as autoridades dessa Parte responsáveis pelo auxílio mútuo internacional ou pela extradição, caso não seja parte integrante dessa ou dessas autoridades.

3 — Cada Parte deverá assegurar que dispõe de pessoal com formação e equipamento de modo a facilitar o funcionamento da rede.

CAPÍTULO IV

Disposições finais

Artigo 36.º

Assinatura e entrada em vigor

1 — A presente Convenção está aberta à assinatura dos Estados membros do Conselho da Europa e dos Estados não membros que tenham participado na sua elaboração.

2 — A presente Convenção está sujeita a ratificação, aceitação ou aprovação. Os instrumentos de ratificação, aceitação ou aprovação deverão ser depositados junto do Secretário-Geral do Conselho da Europa.

3 — A presente Convenção entra em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data em que cinco Estados, incluindo, pelo menos, três Estados membros do Conselho da Europa, tenham manifestado o seu consentimento em ficarem vinculados pela presente Convenção, em conformidade com o disposto nos n.os 1 e 2.

4 — Para qualquer Estado signatário que manifeste posteriormente o seu consentimento em ficar vinculado pela presente Convenção, esta entra em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data em que manifestou o seu consentimento em ficar vinculado pela Convenção, em conformidade com o disposto nos n.os 1 e 2.

Artigo 37.º

Adesão à Convenção

1 — Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa pode, uma vez consultados os Estados Contratantes da Convenção e obtido o seu acordo, convidar qualquer Estado não membro do Conselho que não tenha participado na elaboração da Convenção a aderir à presente Convenção. A decisão deverá ser tomada pela maioria prevista na alínea *d*) do artigo 20.º do Estatuto do Conselho da Europa e por unanimidade de votos dos representantes dos Estados com assento no Comité de Ministros.

2 — Para qualquer Estado que adira à presente Convenção nos termos do n.º 1 do presente artigo, a Convenção entra em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data do depósito do instrumento de adesão junto do Secretário-Geral do Conselho da Europa.

Artigo 38.º

Aplicação territorial

1 — Qualquer Estado pode, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, especificar o ou os territórios aos quais se aplica a presente Convenção.

2 — Qualquer Estado pode, em qualquer momento posterior, mediante declaração dirigida ao Secretário-Geral do Conselho da Europa, estender a aplicação da presente Convenção a qualquer outro território indicado na declaração. Para esse território, a Convenção entra em vigor no primeiro dia do mês seguinte ao termo de um período

de três meses após a data de recepção da declaração pelo Secretário-Geral.

3 — Qualquer declaração feita nos termos dos dois números anteriores, relativamente a qualquer território indicado nessa declaração, pode ser retirada mediante notificação dirigida ao Secretário-Geral. A retirada produz efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção dessa notificação pelo Secretário-Geral.

Artigo 39.º

Efeitos da Convenção

1 — O objectivo da presente Convenção é o de completar os tratados ou os acordos multilaterais ou bilaterais em vigor entre as Partes, incluindo as disposições:

a) Da Convenção Europeia de Extradição, aberta à assinatura a 13 de Dezembro de 1957, em Paris (STE n.º 24);

b) Da Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal, aberta à assinatura a 20 de Abril de 1959, em Estrasburgo (STE n.º 30);

c) Do Protocolo Adicional à Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal, aberto à assinatura a 17 de Março de 1978, em Estrasburgo (STE n.º 99).

2 — Se duas ou mais Partes já tiverem celebrado um acordo ou um tratado sobre as matérias tratadas na presente Convenção ou de outro modo tiverem estabelecido relações entre si sobre tais matérias, ou se assim procederem no futuro, podem também aplicar esse acordo ou tratado ou estabelecer essas relações em substituição da presente Convenção. Contudo, sempre que as Partes estabelecerem relações entre si relativamente às matérias tratadas na presente Convenção de um modo diferente do previsto na presente Convenção, deverão fazê-lo de uma forma que não seja incompatível com os objectivos e os princípios da Convenção.

3 — Nada na presente Convenção deverá afectar outros direitos, restrições, obrigações e responsabilidades de uma Parte.

Artigo 40.º

Declarações

Qualquer Estado pode, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, mediante notificação escrita dirigida ao Secretário-Geral do Conselho da Europa, declarar que se reserva a faculdade de exigir, se for caso disso, um ou mais elementos suplementares tal como previsto nos artigos 2.º, 3.º, na alínea *b*) do n.º 1 do artigo 6.º, no artigo 7.º, no n.º 3 do artigo 9.º e na alínea *e*) do n.º 9 do artigo 27.º

Artigo 41.º

Cláusula federal

1 — Um Estado federal pode reservar-se o direito de assumir as obrigações previstas no capítulo II da presente Convenção que sejam compatíveis com os princípios fundamentais que regem as relações entre o seu governo central e os Estados constituintes ou outras entidades territoriais análogas, desde que se encontre em condições de cooperar ao abrigo do capítulo III.

2 — Ao formular uma reserva nos termos do n.º 1, um Estado federal não a pode utilizar para suprimir ou diminuir de forma substancial as suas obrigações nos termos do capítulo II. Em qualquer caso, deverá dotar-se de meios amplos e eficazes que permitam adoptar essas medidas.

3 — Relativamente às disposições da presente Convenção, cuja aplicação é da competência legislativa de cada um dos Estados constituintes ou de outras entidades territoriais análogas que, por força do sistema constitucional da federação, não estão obrigados a adoptar medidas legislativas, o governo federal deverá informar as autoridades competentes desses Estados das referidas disposições e do seu parecer favorável, encorajando-os a adoptar as medidas adequadas para as aplicar.

Artigo 42.º

Reservas

Qualquer Estado pode, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, mediante notificação escrita dirigida ao Secretário-Geral do Conselho da Europa, declarar que se reserva a faculdade de utilizar a ou as reservas previstas no n.º 2 do artigo 4.º, n.º 3 do artigo 6.º , n.º 4 do artigo 9.º, n.º 3 do artigo 10.º, n.º 3 do artigo 11.º, n.º 3 do artigo 14.º, n.º 2 do artigo 22.º, n.º 4 do artigo 29.º, e n.º 1 do artigo 41.º Nenhuma outra reserva pode ser formulada.

Artigo 43.º

Estatuto e retirada de reservas

1 — Uma Parte que tenha feito uma reserva nos termos do artigo 42.º, pode retirá-la, no todo ou em parte, mediante notificação dirigida ao Secretário-Geral do Conselho da Europa. Essa retirada produz efeitos na data da recepção da referida notificação pelo Secretário-Geral. Se a notificação indicar que a retirada de uma reserva produz efeitos na data nela indicada, e se essa data for posterior à da recepção da notificação pelo Secretário-Geral, a retirada produz efeitos nessa data posterior.

2 — Uma Parte que tenha feito uma reserva nos termos do artigo 42.º, deverá retirá-la, no todo ou em parte, logo que as circunstâncias o permitam.

3 — O Secretário-Geral do Conselho da Europa pode-se informar periodicamente junto das Partes que tenham feito uma ou mais reservas nos termos do artigo 42.º sobre as possibilidades de retirarem essa(s) reserva(s).

Artigo 44.º

Emendas

1 — Qualquer Parte pode propor emendas à presente Convenção, devendo o Secretário-Geral do Conselho da Europa transmiti-las aos Estados membros do Conselho da Europa, aos Estados não membros que tenham participado na elaboração da presente Convenção, bem como a qualquer Estado que a ela tenha aderido ou tenha sido convidado a aderir nos termos do artigo 37.º

2 — Qualquer emenda proposta por uma Parte deverá ser comunicada ao Comité Europeu para os Problemas Criminais (CDPC), o qual deverá submeter a sua opinião sobre essa mesma proposta de emenda à apreciação do Comité de Ministros.

3 — O Comité de Ministros deverá examinar a emenda proposta bem como a opinião do Comité Europeu para os

Problemas Criminais (CDPC) e, após consulta com os Estados não membros que são Partes na presente Convenção, poderá adoptar a referida emenda.

4 — O texto de qualquer emenda adoptada pelo Comité de Ministros em conformidade com o n.º 3 do presente artigo deverá ser comunicado às Partes com vista à sua aceitação.

5 — Qualquer emenda adoptada em conformidade com o n.º 3 do presente artigo entra em vigor no 30.º dia após a data em que todas as Partes tenham comunicado ao Secretário-Geral a sua aceitação.

Artigo 45.º

Resolução de conflitos

1 — O Comité Europeu para os Problemas Criminais do Conselho da Europa deverá ser informado sobre a interpretação e a aplicação da presente Convenção.

2 — Em caso de conflito entre as Partes relativo à interpretação ou aplicação da presente Convenção, as mesmas deverão esforçar-se por resolvê-lo por negociação ou qualquer outro meio pacífico da sua escolha, incluindo a submissão do conflito ao Comité Europeu para os Problemas Criminais, a um tribunal arbitral cujas decisões sejam vinculativas para as Partes no conflito, ou ao Tribunal Internacional de Justiça, conforme acordado entre as Partes interessadas.

Artigo 46.º

Consultas entre as Partes

1 — Quando necessário, as Partes deverão consultar-se periodicamente a fim de facilitar a:

a) Aplicação e execução efectivas da presente Convenção, incluindo a identificação de quaisquer problemas por elas suscitados, bem como os efeitos de qualquer declaração ou reserva feita nos termos da presente Convenção;

b) Troca de informação sobre os desenvolvimentos jurídicos, políticos ou técnicos importantes no domínio da criminalidade informática e da recolha de provas sob a forma electrónica;

c) Avaliação da possibilidade de completar ou alterar a presente Convenção.

2 — O Comité Europeu para os Problemas Criminais (CDPC) deverá ser periodicamente informado do resultado das consultas referidas no n.º 1.

3 — Quando necessário, o Comité Europeu para os Problemas Criminais (CDPC) deverá facilitar as consultas referidas no n.º 1 e adoptar as medidas necessárias para auxiliar as Partes nos seus esforços para completar ou alterar a presente Convenção. O Comité Europeu para os Problemas Criminais (CDPC) deverá, o mais tardar três anos após a entrada em vigor da presente Convenção, em cooperação com as Partes, proceder a uma revisão de todas as disposições da presente Convenção e propor, se for caso disso, as emendas adequadas.

4 — As despesas ocasionadas pela aplicação do disposto no n.º 1, à excepção das que são suportadas pelo Conselho da Europa, deverão ser suportadas pelas Partes, nos termos por elas definidos.

5 — As Partes deverão ser assistidas pelo Secretariado do Conselho da Europa no exercício das suas funções em conformidade com o presente artigo.

Artigo 47.º

Denúncia

1 — Qualquer Parte pode, em qualquer momento, denunciar a presente Convenção mediante notificação dirigida ao Secretário-Geral do Conselho da Europa.

2 — A denúncia produz efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da notificação pelo Secretário-Geral.

Artigo 48.º

Notificação

O Secretário-Geral do Conselho da Europa deverá notificar os Estados membros do Conselho da Europa, os Estados não membros que tenham participado na elaboração da presente Convenção e qualquer Estado que a ela tenha aderido ou tenha sido convidado a aderir:

a) De qualquer assinatura;

b) Do depósito de qualquer instrumento de ratificação, aceitação, aprovação ou adesão;

c) De qualquer data de entrada em vigor da presente Convenção em conformidade com os artigos 36.º e 37.º;

d) De qualquer declaração feita nos termos do artigo 40.º, ou de qualquer reserva nos termos do artigo 42.º;

e) De qualquer outro acto, notificação ou comunicação relacionados com a presente Convenção.

Em fé do que, os abaixo assinados, devidamente autorizados para o efeito, assinaram a presente Convenção.

Feito em Budapeste, em 23 de Novembro de 2001, num único original, nas línguas francesa e inglesa, fazendo ambos os textos igualmente fé. O original deverá ser depositado nos arquivos do Conselho da Europa. O Secretário-Geral do Conselho da Europa deverá remeter uma cópia autenticada a cada um dos Estados membros do Conselho da Europa, aos Estados não membros que tenham participado na elaboração da presente Convenção e a qualquer Estado convidado a aderir a ela.

Resolução da Assembleia da República n.º 89/2009

Aprova as Emendas à Convenção Relativa à Criação do Centro Europeu de Previsão do Tempo a Médio Prazo e a Emenda ao Protocolo sobre Privilégios e Imunidades do Centro Europeu de Previsão do Tempo a Médio Prazo, adoptadas em Reading, na Reunião Extraordinária do Conselho do Centro Europeu, em 22 de Abril de 2005.

A Assembleia da República resolve, nos termos da alínea *i*) do artigo 161.º e do n.º 5 do artigo 166.º da Constituição, aprovar as Emendas à Convenção relativa à Criação do Centro Europeu de Previsão do Tempo a Médio Prazo e a Emenda ao Protocolo sobre Privilégios e Imunidades do Centro Europeu de Previsão do Tempo a Médio Prazo, adoptadas em Reading, na Reunião Extraordinária do Conselho do Centro Europeu, em 22 de Abril de 2005, cujos textos, nas versões autenticadas em língua inglesa e a respectiva tradução em língua portuguesa, se publicam em anexo.

Aprovada em 23 de Julho de 2009.

O Presidente da Assembleia da República, *Jaime Gama.*