

Declassified and approved for publication

2000



COUNCIL OF EUROPE    CONSEIL DE L'EUROPE

**PC-CY (2000) Draft N° 24 REV2**

**EUROPEAN COMMITTEE ON CRIME PROBLEMS**  
**(CDPC)**

**COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE**  
**(PC-CY)**

**Draft Convention on Cyber-crime**  
**(Draft N° 24 REV2)**

Prepared by the Secretariat  
Directorate General I (Legal Affairs)

**DRAFT CONVENTION ON CYBER-CRIME**  
**(Draft N° 24 REV2)**

**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 signatories 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 *cyber-crime*, *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 at 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 cyber-crime and the need to protect legitimate interests in the use and development of information technologies;

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

Convinced that the present Convention is necessary to deter actions 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 the detection, investigation and prosecution of such criminal offences at both the domestic and international level, 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 and the 1966 United Nations International Covenant on Civil and Political Rights which both 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 right to respect for privacy;

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 electronic evidence of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating *cyber*-crimes, including actions of the United Nations, the OECD, the European Union and the G8;

Recalling Recommendation N° 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, Recommendation N° R (88) 2 on piracy in the field of copyright and neighbouring rights as well as Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation N° 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, June 1997), which recommended the Committee of Ministers to support the work carried out by the European Committee on Crime Problems (CDPC) on cyber-crime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as to Resolution N° 3 adopted at the 23<sup>rd</sup> Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as 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 cyber-crime;

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 - 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 inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data [or any other function]<sup>1</sup>;
- 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.
- a. "traffic data" means any computer data relating to a communication by means of a computer system, generated by the computer system that formed part in the chain of communication, indicating its origin, destination, path or route, time<sup>2</sup>, date, size, duration or type of underlying [network] service.

---

<sup>1</sup> The explanatory report should specify that "computer system" refers to the function of data processing and therefore may include any system that is based on such a function, e.g. telecom systems, and that the "inter-connection" referred to in the definition encompasses radio and logical connections.

<sup>2</sup> The reference to 'time' should be understood as time compared to GMT

## **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<sup>3</sup> the access<sup>4</sup> to the whole or any part of a computer system without right<sup>5</sup>. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent<sup>6</sup>, 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<sup>7</sup> 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.

---

3 The interpretation of "intent" should be left to domestic laws, but it should not, where possible, exclude "*dolus eventualis*".

4 This Article is not intended to criminalise regular and common activities inherent in the design of the network, such as sending electronic mail without it having been first solicited by the recipient or normally accessing a web page or ftp ("file transfer protocol") server that has been configured for public access.

5 The expression 'without right' appears in all of the articles of this section and derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their national law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under national law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences).

6 In some countries, interception may be closely related to the offence of unauthorised access to a computer system. In order to ensure consistency of the prohibition and application of the law, countries that require dishonest intent with respect to the offence in article 2 may also require a similar qualifier to attach criminal liability to conduct defined under Article 3.

7 The terms "non-public" relate to the transmission (communication) process and not necessarily to the data transmitted.

#### **Article 4 - Data 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 damaging, deletion, deterioration, alteration<sup>8</sup> or suppression<sup>9</sup> of computer data without right.

#### **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:
    1. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;
    2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessedwith intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and
  - (a) the possession of an item referred to in paragraphs (a)(1) and (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 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 the 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) (2).]

---

<sup>8</sup> The Explanatory Report should specify that ‘Alteration’ also includes tampering with traffic data (spoofing).

<sup>9</sup> The Explanatory Report should clarify that “suppression of data” has two commonly agreed meanings: 1) delete data so that it does no longer exist physically; 2) “render inaccessible”, i.e. prevent someone from gaining access to it while maintaining it.

## *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<sup>10</sup>, 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 by:

- (a) any input, alteration, deletion or suppression of computer data,
- (b) any interference with the functioning of a computer or system,

with the intent of procuring, without right, an economic benefit for *one* self or for another.

## *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<sup>11</sup> the following conduct:
  - (a) offering<sup>12</sup> or making available child pornography through a computer system;
  - (b) distributing or transmitting child pornography through a computer system;

---

<sup>10</sup> The Explanatory Report shall specify that the term “authentic” refers to the issuer of the data, regardless whether the content of the data is true or not.

<sup>11</sup> The Explanatory Report should clarify that the terms “without right” do not exclude legal defenses, excuses or similar relevant principles that relieve a person of responsibility under specific circumstances. Accordingly, conduct undertaken with artistic, medical or similar scientific purposes would not be “without right”. The reference to ‘without right’ would also allow, for example, with respect to paragraph (2) b, that a Party may provide that a person is relieved of criminal responsibility if it is established that the person depicted is not a minor.

<sup>12</sup> The Explanatory Report should specify that ‘offering’ also includes giving information about hyperlinks to child-pornography sites.

- (c) producing child pornography for the purpose of its distribution through a computer system<sup>13</sup>;
  - (d) procuring<sup>14</sup> child pornography through a computer system for oneself or for another;
  - (e) possessing<sup>15</sup> child pornography in a computer system or on a computer-data storage medium.
- 2 For the purpose of paragraph 1 above “child pornography” shall include pornographic material<sup>16</sup> that visually depicts:
- (a) a minor engaged in sexually explicit conduct<sup>17</sup>;
  - (b) a person appearing to be a minor engaged in sexually explicit conduct;
  - (c) realistic images<sup>18</sup> representing a minor engaged in sexually explicit conduct.
1. 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.
2. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(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

---

<sup>13</sup> The Explanatory Report should clarify that this provision by no means is intended to restrict the criminalisation of the distribution, etc, of child pornography to cases making use of a computer system, but the Convention establishes this only as a minimum standard and States are free to go beyond it.

<sup>14</sup> The term “procuring” is intended to cover the downloading of the material referred to in the Article, whether such material will be possessed by the person downloading it or by someone else.

<sup>15</sup> For criminal liability to arise under Article 9, the actor must know that the material offered, made available, distributed, transmitted, produced or possessed is child pornography. It is not sufficient, for example, that a service provider has unknowingly served as a conduit for, or unknowingly hosted a website or newsgroup containing such material. Nothing in this Article requires a service provider to monitor content to avoid criminal liability.

<sup>16</sup> The Explanatory Report should clarify that the term “pornographic material” is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt.

<sup>17</sup> The Explanatory Report should specify that a “sexually explicit conduct” covers at least ***real or simulated***: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor.

<sup>18</sup> The Explanatory Report should clarify that ‘realistic images’ may include morphed images of natural persons.

the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of 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 intentionally, 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 done in Rome (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 intentionally, 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.

#### *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<sup>19</sup> aiding or abetting the commission of any of the offences established in accordance with Articles 2 – 10 of the present Convention.
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 attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1)b and 9(1)c of this Convention.
3. Each State may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

#### **Article 12 – Corporate liability**

---

<sup>19</sup> The Explanatory Memorandum should indicate that Article 11, paragraph 1 contemplates liability for aiding and abetting where the person who commits a crime established in this Convention is aided by another person who shares the mental state required for the commission of the crime. Individuals or legal persons (including service providers) that do not share the objective of committing the crime cannot incur liability through unknowing incidental assistance provided to a criminal actor. The Explanatory Memorandum should also clarify, however, the circumstances under which such individuals or legal persons may be held criminally liable, such as in cases of intentional failure to remove criminal material from a site after having been duly notified.

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable<sup>20</sup> for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, 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.
1. Apart from the cases already provided for in paragraph 1, 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 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 take the necessary measures to ensure that the criminal offences established in accordance with Articles 2 – 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 – Conditions and Safeguards related to the Application of Procedural Measures**

---

<sup>20</sup> Under Articles 11 and 12, a service provider could be liable for criminal actions undertaken for the provider's benefit by agents of the provider, just the same as any other legal person. However, it is important to note that the Article is not intended to impose liability on service providers for the actions of users or customers of their systems. Moreover, this provision does not require or recommend that service providers monitor the transmissions or stored data of users of their systems.

1. The measures adopted in accordance with this Section shall be applied for the purpose of criminal investigations and proceedings<sup>21</sup> concerning the offences established in accordance with Articles 2 – 11 of this Convention, other criminal offences committed by means of a computer system, or the collection of electronic evidence of a criminal offence.
2. The application of the measures adopted shall be subject to the conditions and safeguards provided for under the domestic law of the Party concerned, with due regard for the adequate protection of human rights and, where applicable, the proportionality of the measure to the nature and circumstances of the offence.

### **Article 15 – Scope of Application of Procedural Measures**

1. Except as specifically otherwise provided in Article **21**, each Party shall apply the measures described in this Section to:
  - (a) the offences established in accordance with articles 2-11 of this Convention;
  - (b) other criminal offences committed by means of a computer system; and
  - (c) evidence in electronic form of a criminal offence.
2. **Option 1:** Each Party may, in respect of the offences referred to in paragraphs 1 (b) and (c), 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.
2. **Option 2:** 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 offences referred to in paragraphs 1 (b) and (c) above.

---

<sup>21</sup> The Explanatory Report shall clarify that the reference to “criminal investigations and proceedings” is also intended to clarify the scope of the power in question. The application of such a power in a concrete case involves, however, a specific criminal investigation or proceeding .

*Title 2 - Expedited preservation of stored data*

**Article 16 – Expedited preservation of data stored in a computer system**

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities, in connection with a specific criminal matter, to order or similarly obtain the expeditious preservation of data that has been stored by means of a computer system, in particular where there are grounds to believe that the data is particularly vulnerable<sup>22</sup> to loss or modification.<sup>23</sup>
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored 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 data for an adequate period of time to enable the competent authorities to seek its disclosure.
3. Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the 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 the conditions and safeguards provided for under the domestic law of the Party concerned.<sup>24</sup>

Article 17 – Expedited preservation and disclosure of traffic data

1. In order to enable the undertaking of the procedures referred to in article 16 with respect to the preservation of traffic data concerning a specific communication, each Party shall adopt such legislative and other measures as may be necessary to:
  - (a) ensure the expeditious preservation of that traffic data 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 in order to identify the service providers and the path through which the communication was transmitted.

*Title 3 – Production order*

**Article 18 - Production Order**

- 
- 22 The Explanatory Memorandum should clarify that the term “particularly vulnerable to loss or modification” includes data subject to a short period of retention.
  - 23 The Explanatory Memorandum should clarify that this provision provides only for the power to require preservation pending disclosure of discrete data relating to violations of criminal law upon request in a particular case. It does not mandate retention of all data collected by a service provider or other entity in the course of its activities.
  - 24 The Explanatory Memorandum should indicate that the term “conditions and safeguards” also refers to *the* proportionality test as provided under Article 14, as well as to procedural modalities of the powers defined in articles 16 through 22. The Explanatory Memorandum shall provide additional examples of the kinds of conditions and safeguards Parties may wish to require.

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for the purpose of criminal investigations or proceedings, to order,:
  - (a) a person in its territory to submit<sup>25</sup> specified computer data under this person's control, which is stored in a computer system or a computer-data storage medium; and
  - (b) a service provider offering its services in its territory to submit subscriber information under that service provider's possession or control;
1. The powers and procedures referred to in this article shall be subject to the conditions and safeguards provided for under the domestic law of the Party concerned.
2. For the purpose of this Article, "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 service, other than traffic or content data, by which can be established:
  - i. the type of the communication service used by the subscriber and the technical provisions taken thereto;
  - ii. the subscriber's identity, postal address, telephone number and other access address;
  - iii. any other information on the location of stationary communication equipment, available on the basis of a contract<sup>26</sup>;

#### **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, for the purposes of criminal investigations or proceedings, 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

---

<sup>25</sup> A Party may, by implementing this power in domestic law, require additional criteria and/or conditions, such as "in the manner specified in the order".

<sup>26</sup> The explanatory report should clarify that the reference to a contract should be interpreted in a broad sense and include any kind of relationship on the basis of which a client uses the provider's services.

from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for the purposes of criminal investigations or proceedings, 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; and
  - (d) render inaccessible or remove those computer data in the accessed computer system.
1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order for the purposes of criminal investigations or proceedings any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide all necessary information, as is reasonable, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
2. The powers and procedures referred to in this article shall be subject to the conditions and safeguards provided for under the domestic law of the Party concerned.

### *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, for the purpose of criminal investigations or proceedings, its competent authorities to:
  - (a) collect or record through application of technical means on the territory of that Party, and
  - (b) compel a service provider, within its technical ability, to:
    - (i) collect or record through application of technical means on the territory of that Party, or
    - (ii) 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 required by the established principles of its domestic legal system, a Party may adopt other measures as may be necessary to ensure the real-time**

**collection and recording of traffic data through technical means on its territory, provided that such measures ensure the availability of such data for the purpose of criminal investigations and proceedings.**

- 3. The powers and procedures referred to in this article shall be subject to the conditions and safeguards provided for under the domestic law of the Party concerned.**

### **Article 21 - Interception of content data**

1. Each Party shall adopt such legislative and other measures as may be necessary, for the purpose of criminal investigations or proceedings related to the range of serious offences to be determined by domestic law, to empower its competent authorities to:
  - (a) collect or record through application of technical means on the territory of that Party, and
  - (b) compel a service provider, within its technical ability, to:
    - (i) collect or record through application of technical means on the territory of that Party, or
    - (ii) co-operate and assist the competent authorities in the collection or recording of,  
  
content data, in real-time, of specified communications in its territory<sup>27</sup> transmitted by means of a computer system.
2. Where required by the established principles of its domestic legal system, a Party may adopt other measures as may be necessary to ensure the real-time collection and recording of content data through technical means, provided that such measures ensure the availability of such data for the purpose of criminal investigations and proceedings.
3. The powers and procedures referred to in this article shall be subject to the conditions and safeguards provided for under the domestic law of the Party concerned.

---

<sup>27</sup> The Explanatory Memorandum shall clarify that there is a communication on a country's territory if one of the communicating parties (human beings or computers) is located there.

Article 22 – Obligation of confidentiality

1. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for under Articles 20 and 21.
2. The measures referred to in this article shall be subject to the conditions and safeguards provided for under the domestic law of the Party concerned.

Section 3 - Jurisdiction

**Article 23 - 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 – 11 of this Convention, when the offence is committed :
  - (a) in its territory; or
  - (b) on board a ship flying the flag or registered under the laws 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 State 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 – (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 25, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised in accordance with 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 24 - 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 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 electronic evidence of a criminal offence.

#### ***Title 2 – Principles relating to extradition***

#### **Article 25 - Extradition**

1. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 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. Where an extradition treaty or reciprocal arrangement is in force between two or more Parties, which requires a different minimum penalty for extradition, the minimum penalty provided for in such treaty or reciprocal arrangement shall instead 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 in the case of 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 addresses of each authority<sup>28</sup> responsible for the making to or receipt of a request 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 26 – 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 electronic evidence 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 29 - 35.

3 Each Party shall, in urgent circumstances, accept and respond to mutual assistance requests by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication, with formal confirmation to follow where required by the requested State.

4 Except as otherwise specifically provided [option 1: in Articles 27 – 31 and 33 – 35] [option 2: 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 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 denominates 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 27 (23) - Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

---

<sup>28</sup> Designation of an authority shall not exclude the possibility of using the diplomatic channel. This provision has been limited to situations in which there is no extradition treaty in force between the Parties concerned. Where a bilateral or multilateral extradition treaty is in force between the Parties concerned (such as the 1957 European Convention on Extradition), the Parties will know to whom extradition and provisional arrest requests are to be directed without the necessity of a burdensome registration requirement.

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 10 of this article shall apply. The provisions of this article shall not apply where such agreement, arrangement or legislation is available, 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 that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them 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 so 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.<sup>29</sup>
4. The requested Party may, in addition to conditions or grounds for refusal available under Article 26, paragraph (4), refuse assistance if:
  - (a) the request concerns an offences 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.

1 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.

2 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. 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.

---

<sup>29</sup> The explanatory text should specify that the mere fact that the requested Party's legal system knows no such procedure is not a sufficient ground to refuse to apply the procedure requested by the requesting Party.

3 The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. 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.

- 4 (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 subparagraph (a) 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 – Spontaneous information**

1. A Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information 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 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.

### **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, which is 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 that is seeking the preservation;
  - (b) the offence under investigation and a brief summary of related facts;
  - (c) the stored data to be preserved and its relationship to the offence;
  - (d) the necessity of the preservation; and
  - (e) 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 data.

1. 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.

2. **Option 1:** A Party that requires dual criminality as a condition for the disclosure of data to the requesting Party may, in respect of offences or categories of offences specified in the reservation, other than those established in accordance with Articles 2 – 11 of this Convention, reserve the right to refuse the request for preservation under this Article in cases where it has clear grounds to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

**Option 2:** A Party may, in respect of offences or categories of offences, other than those established in accordance with Articles 2 – 11 of this Convention, require dual criminality as a condition to providing preservation under this Article, where it requires dual criminality as a condition for the disclosure of data to the Requesting Party and it has clear grounds to believe that at the time for disclosure the condition of dual criminality cannot be fulfilled.

**Option 3:** Each State that requires dual criminality as a condition for the disclosure of data to a requesting Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by declaration addressed to the Secretary General of the Council of Europe, declare that in respect of offences or categories of offences specified in such declaration, other than those established in accordance with Articles 2 – 11 of this Convention, it reserves the right to require dual criminality as a condition to providing preservation under this Article.

3. 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.
1. 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.

2. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 60 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 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 under 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 in order 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 application of international instruments, arrangements and laws referred to in article 24, and in accordance with other relevant provisions of this Chapter.
2. The request shall be responded to on an expedited basis where:
  - (a) there are grounds to believe that relevant data is subject to a short period of retention, or is otherwise particularly vulnerable to loss or modification; or
  - (b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

#### **Article 32 (27) – Trans-border access to stored computer data with consent or where publicly available**

A Party may, without obtaining 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 (28bis) - Mutual assistance regarding the real-time collection of traffic data**

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

**Option 1**

2. Each Party may reserve the right to apply the measure referred to in this article only to specified offences or categories of offences, provided that it may not reserve as to the offences established in accordance with articles 2 - 11 of this Convention, and as to offences or categories of offences to which the measure referred to in article 34 may be applied.

**Option 2**

2. Each Party may reserve the right to apply the measure referred to in this article only to specified offences or categories of offences, provided that the range of such offences or categories of offences is not more restricted than that to which the measure referred to in article 34 may be applied. Each Party shall consider restricting its reservation so as to permit application of the measure to the offences established in accordance with articles 2-11 of this Convention.

**Article 34 – Mutual assistance regarding the interception of content data**

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

*Title 3 – 24/7 Network*

**Article 35 (29) - 24/7 Network**

1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of the investigation of criminal offences related to the use of computer systems and data, or for the collection of electronic evidence of any criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:

- (a) providing technical advice;
  - (b) preservation of data pursuant to Articles 29 and 30; and
  - (a) the collection of evidence, giving 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.

### **[Section 3 – Provisions concerning the exchange and protection of information]**

#### Option 1

#### **[[Article 35bis] – Rules on the exchange and protection of information 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 the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such agreement or arrangement is available, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2. The substance of a request for mutual assistance made under this Chapter, or information transferred from one Party to another pursuant to the execution of such a request may be used by the Party to which the information has been transferred only:
- (a) for the purpose of investigations or proceedings stated in the request;
  - (b) for other judicial and administrative proceedings directly related to investigations or proceedings mentioned under paragraph (a) above;
  - (c) for preventing an immediate and serious threat to public security;
  - (d) for any other purpose only with the prior consent of the Party providing the information.
3. Prior to providing the information referred to in paragraph 3, the providing party may request that it be kept confidential or used subject to conditions. If the receiving party cannot comply with such a request, it shall notify the providing Party, which shall then determine whether information should nevertheless be provided. If the receiving Party

accepts the information subject to the conditions, it shall be bound by them. No conditions shall be imposed for cases mentioned under paragraph 2 (c) above.

4. Any Party that transfers information referred to under paragraph 2 may require the Party to which the information has been transferred to explain the use made of such information.]

#### Option 2

#### [Article .. - Confidentiality and Limitation on Use]

- 1. The requesting Party may request that the requested Party not, without the prior consent of the requesting Party, make use of the substance of the request, for purposes other than those for which it was obtained or for criminal investigations or proceedings. If the requested Party cannot comply with the request, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.**
2. The requested Party may request that the requesting Party not, without the prior consent of the requested Party, transmit or use the materials furnished for investigations or proceedings other than those stated in the request. If the requesting Party accepts the materials subject to conditions, it shall be bound by them. If the requesting Party cannot comply with the conditions, it shall promptly inform the requested Party, which shall then determine whether the materials should nevertheless be provided.]

#### Option 3

The text of Option 2 above would be reinserted as subparagraphs into Article 27, paragraph 8

#### Option 4

#### [Article ..] – Confidentiality and Limitation on Use

1. The requested Party may, [in addition to conditions referred to in Article 22 (4),] make the execution of a request made under this Chapter dependent on the condition that the material furnished is  
  
    kept confidential;  
  
    not used for investigations or proceedings other than those stated in the request.
1. If the requesting Party cannot comply with the condition, it shall promptly inform the requested Party, which shall then determine whether the materials should nevertheless be provided.

## 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 their 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 the Contracting States to the Convention, may invite any State not a member of the Council and which has not participated in its elaboration to accede to this Convention, by a decision 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 Party 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 Strasbourg 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 otherwise have established their relations in this matter, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly.
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, as appropriate, one or several additional element(s) as provided for under Article 2, Article 3, Article 6, paragraph 1 (b) Article 7, Article 9, paragraph 3 and Article 27, paragraph 9 (e).

### **Article 41 – [Federal clause]**

*[A federal State may notify the Secretary General that it shall assume obligations under this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities. When making a declaration, a federal State shall provide a statement regarding the nature of its federal system, and of the effect of its federal character on the implementation of the Convention.]*

### **Article 42 – Reservations**

1. *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 6, paragraph 3], Article 9, paragraph 4, Article 10, paragraph 3, Article 11,*

*paragraph 3, Article 15, paragraph 2, Article 23, paragraph 2, Article 29, paragraph 4 [and Article 33, paragraph 2]. No other reservation may be made.*

2. *No State may make reservations to more than [...] of the provisions mentioned in the preceding paragraph.*

#### *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. 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 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.*
1. *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.*
2. *The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the European Committee on Crime Problems (CDPC) and, following consultation of the non-member State Parties to this Convention, may adopt the amendment.*
3. *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.*
4. *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 European Committee on Crime Problems (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

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

- (a) the effective use and implementation of this Convention;
- (b) the exchange of information on significant legal, policy or technological developments pertaining to cyber-crime and the collection of electronic evidence;
- (c) consideration of possible supplementation or amendment of the Convention.

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

3. The European Committee on Crime Problems (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.
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;

any declaration made under Article[s] 40 [and 41] or reservation made in accordance with Article 42;

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 Strasbourg, on .... 200?, 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.