

List of contact points in certain negotiating States



Strasbourg, 27 December 2000

Public version - Declassified
PC-CY (2000) Draft N° 25 REV.

EUROPEAN COMMITTEE ON CRIME PROBLEMS
(CDPC)

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

Draft Convention on Cyber-crime
(Draft N° 25 REV.)

Prepared by the Secretariat
Directorate General I (Legal Affairs)

DRAFT CONVENTION ON CYBER-CRIME
(Draft N° 25 REV.)

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 [as conferred e.g. 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 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, [Recommendation N° R (87) 15 regulating the use of personal data in the police sector] 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 23rd 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 - Definitions¹

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 [...]²;
- 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 the computer system that formed part in the chain of communication, indicating its origin, destination, path or route,³ date, size, duration or type of underlying [network] service.

¹ These definitions still need to be revised.

² 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.

³

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 law⁴ when committed intentionally⁵ the access⁶ to the whole or any part of a computer system without right⁷. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent⁸, 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-public⁹ transmissions

⁴ The Explanatory Report should clarify that a Party may exclude petty or insignificant misconduct from its implementation of the offences defined in Articles 2 – 10, particularly in cases where its domestic legal system does not allow the application of the prosecutorial discretion (opportunity) principle.

⁵ The interpretation of "intent" should be left to domestic laws. It does not, however, exclude "*dolus eventualis*" where such concept exists under domestic law.

⁶ The Explanatory Memorandum should explain that Articles 2 - 5 are not intended to criminalise legitimate and common activities inherent in the design of networks, or common operating or commercial practices, such as, for example, sending electronic mail without it having been first solicited by the recipient; accessing a web page or ftp ("file transfer protocol") server that has been configured for public access; using hypertext links, including deep-links; or employing programs such as "cookies" or "bots" to locate and retrieve information where such programs can be filtered or rejected by the receiving server. In this context, "cookies" should be interpreted as programs that facilitate the processing of communications by storing or retrieving information.

⁷ 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).

⁸ 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.

⁹ The terms "non-public" relate to the transmission (communication) process and not necessarily to the data transmitted.

of computer data to, from or within a computer system¹⁰, 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

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, alteration¹¹ or suppression¹² 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 accessed

¹⁰ The Explanatory Memorandum should clarify that the fact that the notion of “computer systems” may also encompass radio connections (see footnote 1 at article 1) does not mean that a Party is under an obligation to criminalise the interception of any radio transmission which, even though “non public”, takes place in a relatively open and easily accessible manner and therefore can be intercepted, e.g. by radio amateurs.

¹¹ The Explanatory Report should specify that the terms “alteration” and “deletion” also include tampering with packet header data. However, nothing in this Article requires Parties to criminalize modifications to data that facilitate legitimate anonymous communications.

¹² 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.

with intent¹³ that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and

- (b) the possession of an item referred to in paragraphs (a)(1) or (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 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).

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 authentic¹⁴, 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 oneself or for another. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

¹³ “Intent” referred to in the context of paragraphs 1 (a) and (b) should be interpreted as direct intent.

¹⁴ The Explanatory Report shall specify that the term “authentic” refers at minimum to the issuer of the data, regardless whether the content of the data is true or not. In some States, it may also refer to the genuineness of the data.

Title 3 - Content-related offences¹⁵

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 right¹⁶ the following conduct:
 - (a) producing child pornography for the purpose of its distribution through a computer system¹⁷;
 - (b) offering¹⁸ or making available child pornography through a computer system;
 - (c) distributing or transmitting child pornography through a computer system;
 - (d) procuring¹⁹ child pornography through a computer system for oneself or for another;
 - (e) possessing²⁰ child pornography in a computer system or on a computer-data storage medium.

¹⁵ The PC-CY Committee discussed the possibility of including content-related offences other than those defined in Article 9, such as the distribution of racist propaganda through computer systems. While there was a large majority in favour of including the latter as a criminal offence, there was insufficient time for detailed discussions. It was agreed that the PC-CY Committee would suggest to the European Committee on Crime Problems (CDPC) that the drawing up of an additional Protocol to the present Convention be considered as soon as practicable on this issue.

¹⁶ 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.

¹⁷ 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 Parties are free to go beyond it.

¹⁸ The Explanatory Report should specify that ‘offering’ also includes giving information about hyperlinks to child-pornography sites.

¹⁹ 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.

²⁰ A service provider shall not be criminally liable under this Article unless the service provider has, at a minimum, actual knowledge that child pornography is being offered, made available, distributed, transmitted, produced, procured or possessed e.g. through a particular website, chatroom, newsgroup, or similar other storage or communication service. For example, a service provider cannot be held criminally liable when it serves as a conduit for a transmission, such as an electronic mail message, if it does not have actual knowledge that the message contains child pornography. Nothing in this Article requires a service provider to monitor content to avoid criminal liability.

2. For the purpose of paragraph 1 above “child pornography” shall include pornographic material²¹ that visually depicts:
 - (a) a minor engaged in sexually explicit conduct²²;
 - (b) a person appearing to be a minor engaged in sexually explicit conduct;
 - (c) realistic images²³ 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, 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 rights²⁴

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 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 wilfully²⁵, 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

²¹ 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.

²² 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.

²³ The Explanatory Report should clarify that ‘realistic images’ may include morphed images of natural persons.

²⁴ The Explanatory Report should clarify that this article shall in no way be interpreted to extend the protection granted to authors, performers, producers of phonograms, broadcasting organisations or other rightholders to persons that do not meet the criteria for eligibility under domestic law or international agreement.

²⁵ The term “wilfully” is used in Article 10 instead of “intentionally”, in both paragraphs 1 and 2, on the ground that “wilfully” is used in article 61 of the TRIPS agreement (governing the obligation to criminalise).

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 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 circumstances²⁶, 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 intentionally²⁷ 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) a 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

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable 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;

²⁶ The Explanatory Report shall include some examples of the kind of circumstances, such as those related to rental rights and web-broadcasting, which Parties may invoke so as not to impose criminal liability under paragraphs 1 and 2 of this Article.

²⁷ The Explanatory Memorandum should indicate that individuals or legal persons (including service providers) that do not share the objective of committing the crime cannot incur liability.

- (c) an authority to exercise control within the legal person.
2. 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 liable²⁸ 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 – 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 otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to:
 - (a) the criminal offences established in accordance with articles 2-11 of this Convention;
 - (b) other criminal offences committed by means of a computer system; and

²⁸ Article 12 is intended to impose liability on corporations, associations, organisations and similar legal persons for the criminal actions undertaken by a person in a leading position within such legal person, where undertaken for the benefit of that legal person. Article 12 does not impose liability on a legal person for the actions of customers, users, or other third persons. Article 12 also contemplates liability where such a leading person fails to supervise or control an agent of the legal person, where such failure facilitates the commission by that agent of one of the offences established in the Convention. It is left to a Party's national law whether

- (c) the collection of evidence in electronic form of a criminal offence.
3. 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 so as to enable the broadest application of the measure referred to in Article 20.

Article 15 – Conditions and Safeguards

The establishment, implementation and application of the powers and procedures provided for in this Section shall be subject to the conditions and safeguards provided for under the domestic law of each Party concerned, with due regard for the adequate protection of human rights, in particular as provided in applicable international human rights instruments²⁹, and, where applicable, the proportionality³⁰ of the power or procedure to the nature and circumstances of the offence.

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 vulnerable³¹ to loss or modification.³²
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 an

²⁹ The Explanatory Report should clarify that these international instruments include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols, as well as the 1966 International Covenant on Civil and Political Rights.

³⁰ In determining the proportionality of a measure, Parties may also wish to consider the economic impact of the measure. In this regard, Parties should consider implementing means of mitigating economic burdens on innocent third parties, such as service providers, incurred as a result of measures taken.

³¹ The Explanatory Memorandum should clarify that the term “particularly vulnerable to loss or modification” includes data saved for a short period of time.

³² The Explanatory Memorandum should clarify that this provision provides only for the power, in a particular case in relation to a criminal offence, to require preservation pending the taking of measures to obtain discrete data and disclose it. It does not mandate retention of all data collected by a service provider or other entity in the course of its activities. It should also be made clear that the retention of traffic data and the preservation of specific traffic data are different concepts.

adequate period of time, as necessary, 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 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 submit³³ 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;
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

³³ 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".

3. 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 users of its service, other than traffic or content data, by which can be established:
 - i. the type of the communication service used, the technical provisions taken thereto and the period of service;
 - ii. the user’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;
 - iii. 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) 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, such 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; and
 - (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 reasonable³⁴, 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 application of technical means on the territory of that Party, and
 - (b) compel a service provider, within its existing technical capability³⁵, 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 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 in its territory through application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures³⁶ as may be necessary to oblige a service provider to keep confidential³⁷ the fact of and any information about the execution of any power provided for in this Article.

³⁴ The reference to the “reasonable” nature of the measure should be interpreted as not requiring those subject to it to collect information other than that which is already available to them, nor as requiring anyone other than those who have a direct relationship to the computer system to assist.

³⁵ The phrase “within existing technical capability” indicates that this paragraph (and Article 21(1)(b)) should not be implemented in a manner that requires service providers to acquire or develop new technical abilities in order to collect and record data or perform other related activities at the request of a Party.

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 application of technical means on the territory of that Party, and
 - (b) compel a service provider, within its existing technical capability³⁸, 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 territory³⁹ 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 of specified communications in its territory through application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures⁴⁰ as may be necessary to oblige a service provider to keep confidential⁴¹ the fact of and any information about the execution of any power provided for in this Article.

³⁶ If a Party is able to ensure the confidentiality of the data held by service providers on the basis of other domestic legal provisions, such as the prohibition of “obstruction of justice”, this will suffice for the implementation of this Article.

³⁷ The Explanatory Report should specify that domestic laws will need to determine the period of time for which the confidentiality of the measures can be ordered.

³⁸ See footnote 36.

³⁹ The Explanatory Memorandum should clarify that there is a communication on a country's territory if one of the communicating parties (human beings or computers) is located there.

⁴⁰ See footnote 37.

⁴¹ The Explanatory Report should specify that domestic laws will need to determine the period of time for which the confidentiality of the measures can be ordered.

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

Article 22 – incorporated into Articles 20 and 21

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
 - (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 evidence in electronic form 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 authority⁴² 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 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 - 35.
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communications, 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 solely on the ground that the request concerns an offence which it considers a fiscal offence.

⁴² 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.

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 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.

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 10 of this article shall apply. The provisions of this article shall not apply where such treaty, 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.⁴³
 4. The requested Party may, in addition to 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.
 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. 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.
 8. 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.
 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).

⁴³ The explanatory report 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.

- (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.

⁴⁴[**Article 27 bis – 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, is available 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 furnishing 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.⁴⁵
3. If the requesting Party cannot comply with a condition referred to in para. 2, it shall promptly inform the other Party, which shall then determine whether the information is nevertheless provided. When the requesting Party accepts the condition, it shall be bound by it.⁴⁶

⁴⁴ The text of this provision needs further improving as yet there is no full consensus on the current text.

⁴⁵ Under the fundamental principles of many States, if the material furnished is evidence exculpatory to an accused person, it must be disclosed to the defense or a judicial authority. In this situation, it is not possible to ensure confidentiality or limit use to the investigation or proceeding for which mutual assistance was sought. In addition, most material furnished under mutual assistance regimes is intended for further dissemination, such as for use at trial, normally a public proceeding. Once such disclosure takes place, the requesting Party's authorities lose control over the use of the material, which has essentially passed into the public domain. Also, as a practical and policy matter, in this situation there appears to be no basis for further limitations. It was agreed that in these two situations the use limitation in this Article would not apply.

⁴⁶ In the Explanatory Note it will be made clear that this article is without prejudice to Article 27. [It is understood that restrictions on the use of information in the application of these articles cannot have the effect to hamper mutual assistance substantively. Article 27bis does not exclude the possibility of adding other conditions of a data protection nature on the basis of Article 27, paragraph 6.]

4. Any Party that furnishes information or material subject to a condition referred to in para. 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 (24) - 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 that is the subject of a criminal investigation or proceeding and a brief summary of related facts;
 - (c) the stored computer data to be preserved and its relationship to the offence;
 - (d) any available information to identify 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 the data may, in respect of offences 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 reason 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 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.

3. The request shall be responded to on an expedited basis where:
 - (a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
 - (b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without 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 - 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.
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 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 - 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 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:

- (a) provision of technical advice;
 - (b) preservation of data pursuant to Articles 29 and 30; and
 - (c) 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.

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 with and obtaining the unanimous consent of 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. 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 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 additional elements 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.⁴⁷]

⁴⁷ The explanatory memorandum will indicate that Article 41 is intended to recognise that minor variations in coverage may occur as a result of the domestic law and practice of a Party that is a federal state. Such

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 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 2, Article 23, paragraph 2, Article 29, paragraph 4. 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. 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.

powers in criminal justice matters between the central government and its constituent states or territorial entities. For example, in the United States under its Constitution and fundamental principles of federalism, federal criminal legislation generally regulates conduct based on its effects on interstate or foreign commerce, while matters of minimal or purely local concern are traditionally regulated by the constituent states. This approach to federalism still provides for broad coverage of illegal conduct encompassed by this convention under US federal criminal law, but recognises that the constituent states would continue to regulate conduct that has only minor impact or is purely local in character. In some instances within that narrow category of conduct regulated by state but not federal law, a constituent state may not provide for a measure that would otherwise fall within the scope of this Convention. For example, an attack on a stand-alone personal computer, or network of computers linked together in a single building, may only be criminal if provided for under the law of the state in which the attack took place; however, the attack would be a federal offense if access to the computer took place through the Internet, since the use of the Internet provides the effect on interstate or foreign commerce necessary to invoke federal law. The implementation of this convention through United States federal law as described

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 European Committee on Crime Problems (CDPC) and, following consultation with the non-member State 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 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

1. 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 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 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;
- (d) any declaration made under Article[s] 40 [and 41] 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 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.