REPUBBLICA DI SAN MARINO

DECRETO CONSILIARE 21 gennaio 2019 n.8

Noi Capitani Reggenti
la Serenissima Repubblica di San Marino

Visto il combinato disposto dell'articolo 5, comma 3, della Legge Costituzionale n.185/2005 e dell'articolo 11, comma 2, della Legge Qualificata n.186/2005;
Vista la delibera del Consiglio Grande e Generale n.4 del 17 gennaio 2019;
ValendoCi delle Nostre Facoltà;
Promulghiamo e mandiamo a pubblicare:

RATIFICA DELLA CONVENZIONE DEL CONSIGLIO D'EUROPA SULLA CRIMINALITA' INFORMATICA E DEL PROTOCOLLO ADDIZIONALE ALLA CONVENZIONE SULLA CRIMINALITA' INFORMATICA, RELATIVO ALL'INCRIMINAZIONE DI ATTI DI NATURA RAZZISTA E XENOFOBICA COMMESI A MEZZO DI SISTEMI INFORMATICI

Articolo Unico

Piena ed intera esecuzione è data alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Allegato A), fatta a Budapest il 23 novembre 2001 e al Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici (Allegato B), fatto a Strasburgo il 28 gennaio 2003, a decorrere dall'entrata in vigore della Convenzione e del Protocollo, in conformità a quanto disposto dall'articolo 36 della Convenzione e dall'articolo 10 del Protocollo.

Dato dalla Nostra Residenza, addì 21 gennaio 2019/1718 d.F.R

I CAPITANI REGGENTI
Mirco Tomassoni – Luca Santolini

IL SEGRETARIO DI STATO
PER GLI AFFARI INTERNI
Guerrino Zanotti

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

European Treaty Series - No. 185

Convention on Cybercrime

Budapest, 23.XI.2001

Preamble

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

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

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

c "service provider" means:

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

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

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

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

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

Article 3 – Illegal interception

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

Article 4 – Data interference

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

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

Article 5 – System interference

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

Article 6 – Misuse of devices

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

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

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

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

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

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

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

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

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

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

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system,

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

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

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

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

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

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.

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

Article 10 – Offences related to infringements of copyright and related rights

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

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

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

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

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

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

Article 13 – Sanctions and measures

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

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

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

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

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

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

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

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

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

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

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

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

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

Article 15 – Conditions and safeguards

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

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

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

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

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

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

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

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

Article 17 – Expedited preservation and partial disclosure of traffic data

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

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

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

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

Title 3 – Production order

Article 18 – Production order

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

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

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

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

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

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

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

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

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

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

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

b a computer-data storage medium in which computer data may be stored

in its territory.

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

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

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

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

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

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

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

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

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

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

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

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

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

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

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

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

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

Article 21 – Interception of content data

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

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

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

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

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

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

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

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

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

Section 3 – Jurisdiction

Article 22 – Jurisdiction

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

a in its territory; or

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

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

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

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

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

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

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

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

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

Title 2 – Principles relating to extradition

Article 24 – Extradition

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

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

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

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

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

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

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

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

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

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

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

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

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

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

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

Article 26 – Spontaneous information

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

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

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

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

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 28 – Confidentiality and limitation on use

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

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

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

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

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

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

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

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

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

a the authority seeking the preservation;

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

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

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

e the necessity of the preservation; and

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

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

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

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

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

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

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

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

Article 30 – Expedited disclosure of preserved traffic data

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

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

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

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

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

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

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

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

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

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

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

A Party may, without the authorisation of another Party:

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

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

Article 33 – Mutual assistance regarding the real-time collection of traffic data

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

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

Article 34 – Mutual assistance regarding the interception of content data

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

Title 3 – 24/7 Network

Article 35 – 24/7 Network

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

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

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

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

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

Article 40 – Declarations

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

Article 41 – Federal clause

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

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

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

Article 42 – Reservations

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

Article 43 – Status and withdrawal of reservations

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

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

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

Article 44 – Amendments

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

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

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

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

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

Article 45 – Settlement of disputes

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

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

Article 46 – Consultations of the Parties

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

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

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

c consideration of possible supplementation or amendment of the Convention.

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

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

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

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

Article 47 – Denunciation

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

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

Article 48 – Notification

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

a any signature;

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

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

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

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

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

CONVENZIONE DEL CONSIGLIO D'EUROPA SULLA CRIMINALITÀ INFORMATICA

Budapest, 23.XI.2001

PREAMBOLO

GLI STATI MEMBRI DEL CONSIGLIO D'EUROPA E GLI ALTRI STATI FIRMATARI

considerando che lo scopo del Consiglio d'Europa è quello di ottenere un legame più stretto fra i propri membri;

riconoscendo l'interesse ad intensificare la collaborazione con gli altri Stati parte in questa Convenzione;

convinti della necessità di perseguire, come questione prioritaria, una politica comune in campo penale finalizzata alla protezione della società contro la criminalità informatica, adottando una legislazione appropriata e sviluppando la cooperazione internazionale;

consci dei profondi cambiamenti dipendenti dall'introduzione della tecnologia digitale, dalla convergenza e costante globalizzazione delle reti informatiche;

preoccupati dei rischi che le reti informatiche e le informazioni in formato elettronico possano anche essere utilizzate per commettere reati e che le prove connesse a tali reati possano essere conservate e trasferite tramite queste reti;

riconoscendo la necessità della cooperazione tra gli Stati e le società private nella lotta alla criminalità informatica e la necessità di tutelare gli interessi legittimi nell'uso e nello sviluppo delle tecnologie informatiche;

ritenendo che una lotta sostanziale alla criminalità informatica richiede una crescente, veloce e ben funzionante cooperazione internazionale in campo penale;

convinti che la presente Convenzione sia necessaria come deterrente per azioni dirette contro la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati informatici, così come per l'uso improprio di questi sistemi, reti ed informazioni, attraverso la criminalizzazione di questi comportamenti, come descritto nella presente Convenzione, e attraverso l'adozione di poteri sufficienti per combattere realmente questi reati, facilitando la loro individuazione, investigazione e l'esercizio dell'azione penale a livello sia nazionale che internazionale e prevedendo accordi per una cooperazione internazionale più veloce e affidabile;

tenendo presente la necessità di garantire un equo bilanciamento tra l'interesse per l'azione repressiva ed il rispetto dei diritti umani fondamentali come previsto nella Convenzione del Consiglio d'Europa del 1950 per la Tutela dei Diritti Umani e le Libertà Fondamentali, la Convenzione Internazionale delle Nazioni Unite del 1966 sui Diritti Civili e Politici e gli altri trattati applicabili sui diritti umani che riaffermano il diritto di ciascuno di avere opinioni senza condizionamenti, come anche il diritto alla libertà di espressione, incluso il diritto di cercare, ricevere, e trasmettere informazioni e idee di ogni tipo, senza limiti di frontiere, e il diritto al rispetto della *privacy*;

consapevoli anche del diritto alla tutela delle informazioni personali, ad esempio, in base alla Convenzione del 1981 del Consiglio d'Europa per la tutela degli Individui con riguardo alla gestione automatizzata dei dati personali;

tenuto conto della Convenzione delle Nazioni Unite del 1989 sui diritti dei minori e della Convenzione del 1999 dell'Organizzazione Internazionale del Lavoro sulle peggiori forme di lavoro minorile;

tenendo presente la Convenzione del Consiglio d'Europa sulla cooperazione in campo penale ed anche i trattati simili che esistono tra gli Stati membri del Consiglio d'Europa e gli altri Stati, e mettendo in evidenza che la presente Convenzione viene intesa come integrazione di queste convenzioni al fine di rendere più efficienti le indagini e l'azione penale su reati commessi in materia di sistemi informatici ed informazioni e consentire la raccolta di prove di un reato in forma elettronica;

accogliendo con favore i recenti sviluppi, quali la migliore conoscenza in campo internazionale e la cooperazione nella lotta alla criminalità informatica, inclusa l'azione intrapresa dalle Nazioni Unite, l'OECD, l'Unione Europea e il G8;

richiamando le Raccomandazioni del Comitato dei Ministri No. R (85) 10 riguardante la concreta applicazione della Convenzione Europea sulla Mutua Assistenza Legale in Campo Penale nel rispetto delle Rogatorie per l'intercettazione delle telecomunicazioni, No. R (88) 2 sulla pirateria nel campo del *copyright* e il diritto dei vicini, No. R (87) 15 che regola l'uso di informazioni personali da parte delle forze dell'ordine, No. R (95) 4 sulla protezione dei dati personali nell'area dei servizi delle telecomunicazioni, con particolare riguardo ai servizi telefonici, come anche la No. R (89) 9 sui crimini connessi all'uso di computer, prevedendo delle linee giuda per le legislazioni nazionali riguardanti la definizione di alcuni crimini informatici e No. R (95) 13 riguardante problemi di diritto procedurale penale collegati con l'*information technology*;

avendo riguardo alla Risoluzione No. 1 adottata dai Ministri della Giustizia Europei nel corso della loro 21° Conferenza (Praga, 10 e 11 Giugno 1997), che raccomandava che il Comitato dei Ministri supportasse il lavoro sulla criminalità informatica svolto dal Comitato Europeo sui Problemi Penali (CDPC) al fine di rendere le legislazioni dei singoli Paesi più simili tra loro e di consentire l'uso di sistemi pratici nelle indagini su questi reati, così come la Risoluzione No. 3 adottata alla 23° Conferenza dei Ministri Europei della Giustizia (Londra, 8 e 9 Giugno 2000) che incoraggia le parti a proseguire nei loro sforzi volti a trovare soluzioni adeguate per consentire al maggior numero di Stati di divenire parti della Convenzione e riconoscendo la necessità di un rapido ed efficiente sistema di cooperazione internazionale che prenda nel dovuto conto la richiesta specifica di lotta contro la criminalità informatica;

avendo anche riguardo al Piano d'Azione dei Capi di Stato e dei Governi del Consiglio d'Europa elaborato in occasione del loro Secondo Summit (Strasburgo, 10 e 11 Ottobre 1997) per cercare risposte comuni allo sviluppo delle nuove tecnologie basate su *standards* e valori propri del Consiglio d'Europa,

HANNO CONVENUTO QUANTO SEGUE

CAPITOLO I
USO DEI TERMINI

Articolo 1
Definizioni

Ai fini della presente Convenzione:

a. "*sistema informatico*" indica qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati;

b. "*dati informatici* " indica qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione;

c. "*service provider*" (fornitore di servizi), indica:

1. qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico;

2. qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio;

d. "*trasmissione di dati*" indica qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio.

CAPITOLO II
PROVVEDIMENTI DA ADOTTARE A LIVELLO NAZIONALE

SEZIONI I
DIRITTO PENALE SOSTANZIALE

TITOLO I
REATI CONTRO LA RISERVATEZZA, L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI E DEI SISTEMI INFORMATICI

Articolo 2
Accesso Illegale ad un sistema informatico

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per sanzionare come reato in base alla propria legge nazionale l'accesso all'intero sistema informatico o a parte di esso senza autorizzazione.

Una Parte può richiedere che il reato venga commesso violando misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer o con altro intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico.

Articolo 3

Intercettazione abusiva

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale l'intercettazione senza autorizzazione, fatta con strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico, incluse le emissioni elettromagnetiche da un sistema informatico che ha tali dati informatici. Una Parte può richiedere che il reato venga commesso con intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico.

Articolo 4

Attentato all'integrità dei dati

1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale il danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici senza autorizzazione.
2. Ogni Parte può riservarsi il diritto di richiedere che la condotta descritta nel paragrafo 1. sia di grave danno.

Articolo 5

Attentato all'integrità di in un sistema

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale il serio impedimento, senza alcun diritto, del funzionamento di un sistema informatico tramite l'introduzione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici.

Articolo 6

Abuso di apparecchiature

1 Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commessi intenzionalmente e senza autorizzazione:

a. la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o l'utilizzabilità in altro modo di:

1. un'apparecchiatura, incluso un programma per computer, destinato o utilizzato principalmente al fine di commettere un qualsiasi reato in base agli articoli da 2 a 5 di cui sopra;

2. una *password* di un computer, un codice d'accesso, o informazioni simili con le quali l'intero sistema informatico o una sua parte sono accessibili, con l'intento di commettere qualsiasi reato in base agli articoli da 2 a 5 di cui sopra;

b. il possesso di uno elemento di cui ai sopra citati paragrafi a. 1. o 2., con l'intento di utilizzarlo allo scopo di commettere qualche reato in base agli articoli da 2 a 5. Una Parte può richiedere per legge che vi sia il possesso di un certo numero di tali elementi perché vi sia una responsabilità penale.

2. Questo articolo non va interpretato nel senso di prevedere una responsabilità penale laddove la produzione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o l'utilizzazione in altro modo o il possesso di cui al paragrafo 1. di questo articolo, non avvenga allo scopo di commettere un reato in base agli articoli da 2 a 5 di questa Convenzione, come anche per il collaudo autorizzato o la protezione di un sistema informatico.

3. Ogni Parte può riservarsi il diritto di non applicare il paragrafo 1. di questo articolo, purché tale riserva non concerna la vendita, la distribuzione o l'utilizzazione in altro modo degli elementi riferiti al paragrafo 1 a. 2. di questo articolo.

TITOLO II
REATI INFORMATICI

Articolo 7
Falsificazione informatica

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commessi intenzionalmente e senza alcun diritto, l'introduzione, l'alterazione, il possesso o la soppressione di dati informatici derivanti da dati non autentici con l'intento che essi siano presi in considerazione o utilizzati con fini legali come se fossero autentici, senza avere riguardo al fatto che i dati siano o meno direttamente leggibili o intelligibili. Una Parte può richiedere che il reato venga commesso fraudolentemente, o con un intento illegale paragonabile, perché vi sia una responsabilità penale.

Articolo 8
Frode informatica

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso intenzionalmente e senza alcun diritto, il cagionare un danno patrimoniale ad altra persona:

a. con ogni introduzione, alterazione, cancellazione o soppressione di dati informatici;

b. con ogni interferenza nel funzionamento di un sistema informatico, con l'intento fraudolento o illegale di procurare, senza alcun diritto, un beneficio economico per se stesso o altri.

TITOLO II
REATI RELATIVI AI CONTENUTI

Articolo 9
Reati relativi alla pornografia infantile

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesse intenzionalmente e senza alcun diritto:

a. la produzione di pornografia infantile allo scopo della sua diffusione attraverso un sistema informatico;

b. l'offerta o la messa a disposizione di pornografia infantile attraverso un sistema informatico;

c. la distribuzione o la trasmissione di pornografia infantile attraverso un sistema informatico;

d. il procurare pornografia infantile attraverso un sistema informatico per se stessi o altri;

e. il possesso di pornografia infantile attraverso un sistema informatico o uno strumento di archiviazione di dati informatici.

2. Ai fini del Paragrafo 1. di cui sopra, l'espressione " pornografia infantile " include il materiale pornografico che raffigura:

a. un minore coinvolto in un comportamento sessuale esplicito;

b. un soggetto che sembra essere un minore coinvolto in un comportamento sessuale esplicito;

c. immagini realistiche raffiguranti un minore coinvolto in un comportamento sessuale esplicito;

3. Ai fini del Paragrafo 2. di cui sopra, il termine "minore" include tutte le persone sotto i 18 anni di età. Una Parte può comunque richiedere un età minore, che non potrà essere inferiore ai 16 anni.

4. Ogni Parte può riservarsi il diritto di non applicare in tutto o in parte il paragrafo 1., sottoparagrafi d. ed e., e 2, sottoparagrafi b.e c.

TITOLO IV
REATI CONTRO LA PROPRIETÀ INTELLETTUALE E DIRITTI COLLEGATI

Articolo 10
Reati contro la proprietà intellettuale e diritti collegati

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale la violazione della proprietà intellettuale, come definita in base alla legge di quella Parte, tenendo fede agli obblighi che ha assunto in base al *Paris Act* del 24 luglio 1971 che ha modificato la Convenzione di Berna sulla protezione delle opere letterarie e artistiche, l'Accordo sugli aspetti commerciali dei diritti sulla proprietà intellettuale e il Trattato OMPI sulla proprietà intellettuale, con l'eccezione di tutti i diritti morali conferiti da queste convenzioni, se tali atti sono commessi deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico.

2. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale la violazione di diritti connessi come definiti dalla legge di quello Stato Parte, tenendo fede agli obblighi che ha assunto in base alla Convenzione Internazionale per la protezione degli artisti, interpreti ed esecutori, produttori di fonogrammi e organismi di radiodiffusione (Convenzione di Roma), all'Accordo sugli aspetti commerciali dei diritti sulla proprietà intellettuale e il Trattato OMPI sull'interpretazione e l'esecuzione e i fonogrammi, con l'eccezione di tutti i diritti morali conferiti da queste convenzioni, se tali atti sono commessi deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico.

3. Una Parte può riservarsi il diritto di non imporre la responsabilità penale in base ai paragrafi 1. e 2. di questo articolo in determinate circostanze, a condizione che altri rimedi efficaci siano disponibili e che tale riserva non deroghi agli obblighi internazionalmente

assunti da questa Parte in applicazione degli strumenti internazionali menzionati nei paragrafi 1. e 2. di questo articolo.

TITOLO V
ALTRE FORME RESPONSABILITÀ E SANZIONI

Articolo 11
Tentativo e complicità

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, ogni complicità quando sia commessa intenzionalmente in vista della perpetrazione di un'infrazione di cui agli articoli da 2 a 10 della presente Convenzione, con l'intento che tale reato venga commesso.
2. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso volontariamente, il tentativo di commettere ogni tipo di reato in base agli articoli da 3 a 5, 7,8,9.1 a. e c. della presente Convenzione.
3. Ogni parte può riservarsi il diritto di non applicare, in tutto o in parte, il paragrafo 2 di questo articolo.

Articolo 12
Responsabilità delle Persone Giuridiche

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie affinché le persone giuridiche possano essere ritenute responsabili di un reato in base a questa Convenzione commesso per loro conto da una persona fisica che agisca sia individualmente che come membro di un organo di una persona giuridica che eserciti un potere di direzione al suo interno, nei termini che seguono:
   a. un potere di rappresentanza della persona giuridica;
   b. un'autorità per assumere decisioni nel nome della persona giuridica;
   c. un'autorità per esercitare un controllo all'interno della persona giuridica.
2. In aggiunta ai casi già previsti nel paragrafo 1. di questo articolo, ogni Parte deve adottare le misure necessarie affinché una persona giuridica possa essere ritenuta responsabile se la mancanza di sorveglianza o controllo di una persona fisica di cui al paragrafo 1. ha reso possibile la commissione di reati previsti al paragrafo 1. per conto della persona giuridica da parte di una persona fisica che agisca sotto la sua autorità.

3. Secondo i principi giuridici della Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa.

4.Questa responsabilità è stabilita senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso il reato.

Articolo 13

Sanzioni e Strumenti

1.Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie affinché i reati previsti in applicazione degli articoli da 2 a 11 possano essere puniti con sanzioni effettive, proporzionate e dissuasive, che includano la privazione della libertà.

2.Ogni parte deve assicurarsi che le persone giuridiche ritenute responsabili in base all'articolo 12 siano assoggettate a sanzioni penali o non penali effettive, proporzionate e dissuasive o ad altre misure, incluse sanzioni pecuniarie.

SEZIONE II
DIRITTO PROCEDURALE

TITOLO I
DISPOSIZIONI COMUNI

Articolo 14

Ambito di applicazione delle disposizioni procedurali

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire i poteri e le procedure previste in questa Sezione per indagini o procedimenti penali specifici.

2. Salvo contraria disposizione risultante all'articolo 21, ogni Parte deve applicare i poteri e le procedure menzionati nel paragrafo 1.:

a. ai reati previsti in conformità agli articoli da 2 a 11 della presente Convenzione;

b. a tutti gli altri reati commessi attraverso un sistema informatico;

c. all'insieme delle prove elettroniche di un reato.

3. a. Ogni Parte si può riservare il diritto di applicare le misure di cui all'articolo 20 solamente ai reati o alle categorie di reati specificati nella riserva, purché l'ambito di tali reati o categorie di reato non sia più ristretto di quello dei reati ai quali la Parte applica le misure di cui all'articolo 21. Ogni Pare dovrà considerare di ridurre questo tipo di riserva in modo da consentire l'applicazione più ampia possibile delle misure di cui all'articolo 20.

b. Qualora una Parte, a causa dei limiti previsti nella propria legislazione al momento dell'adozione della presente Convenzione, non è in grado di applicare le misure previste agli articoli 20 e 21 alle comunicazioni trasmesse in un sistema informatico di un *service provider* (fornitore di servizi), il cui sistema:

i. è operativo a vantaggio di un gruppo definito di utenti, e

ii. non utilizza reti di comunicazione pubblica e non è connesso con un altro sistema informatico, sia pubblico o che privato,

questa Parte si può riservare il diritto di non applicare queste misure a tali comunicazioni. Ogni Parte dovrà prevedere di ridurre tale riserva per consentire la più amplia applicazione possibile delle misure di cui agli articoli 20 e 21.

Articolo 15

Condizioni e tutele

1. Ogni Parte deve assicurarsi che l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste in questa sezione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un'adeguata tutela dei diritti umani e delle libertà, in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e agli altri strumenti internazionali applicabili in materia di diritti umani, e che deve considerare il principio di proporzionalità.

2. Quando sia il caso, avuto riguardo alla natura del potere o della procedura, queste condizioni e tutele devono includere, fra l'altro, una supervisione giudiziaria o di altra natura purché indipendente, dei motivi che giustifichino l'applicazione e la limitazione del campo di applicazione e della durata del potere o procedura.

3. Nella misura in cui ciò sia rispondente all'interesse pubblico e, in particolare, alla buona amministrazione della giustizia, ogni Parte deve considerare l'impatto dei poteri e delle procedure di questa sezione sui diritti, le responsabilità e gli interessi legittimi dei terzi.

TITOLO II
CONSERVAZIONE RAPIDA DI DATI INFORMATICI IMMAGAZZINATI

Articolo 16
Conservazione rapida di dati informatici immagazzinati

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per consentire alle competenti autorità di ordinare o ottenere in altro modo la protezione rapida di specifici dati informatici, inclusi i dati sul traffico, che sono stati conservati attraverso un sistema informatico, in particolare quando vi è motivo di ritenere che i dati informatici siano particolarmente vulnerabili e soggetti a cancellazione o modificazione.

2. Quando una Parte rende effettive le previsione di cui al precedente paragrafo 1. attraverso l'ordine ad un soggetto di conservare specifici dati informatici immagazzinati che siano in suo possesso o sotto il suo controllo, la Parte deve adottare le misure legislative e di altra natura che siano necessarie per obbligare tale soggetto a proteggere e mantenere l'integrità di quei dati informatici per il periodo di tempo necessario, per un massimo di novanta giorni, per consentire alle autorità competenti di ottenere la loro divulgazione. Una Parte può prevedere che tale ordine possa essere successivamente rinnovato.

3. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per obbligare il custode o la persona incaricata di conservare i dati informatici di mantenere il segreto sulla procedura intrapresa per il periodo di tempo previsto dal proprio diritto interno.

4. I poteri e le procedure di cui al presente articolo devono essere soggetti agli articoli 14 e 15.

Articolo 17
Conservazione e divulgazione rapide di dati relativi al traffico

1. Al fine di assicurare la conservazione dei dati relativi al traffico in applicazione di quanto previsto all'articolo 16 ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per:

a. assicurare che la conservazione dei dati relativi al traffico sia disponibile nonostante uno o più fornitori di servizi siano stati coinvolti nella trasmissione di tale comunicazione; e

b. assicurare la rapida trasmissione all'autorità competente della Parte, o al soggetto designato da tale autorità, di una quantità di dati relativi al traffico sufficiente per consentire alla Parte di identificare il fornitore di servizi e la via attraverso la quale la comunicazione fu trasmessa.

2. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

TITOLO III
INGIUNZIONE DI PRODURRE

Articolo 18
Ingiunzione di produrre

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per consentire alle autorità competenti di ordinare:

a. ad un soggetto nel proprio territorio di trasmettere specifici dati informatici nella propria disponibilità o controllo, che siano immagazzinati in un sistema informatico in un supporto informatico per la conservazione di dati; e

b. a un fornitore di servizi che offre le proprie presatazioni nel territorio della Parte di fornire i dati in proprio possesso o sotto il suo controllo relativi ai propri abbonati e concernenti tali servizi.

2. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

3. Ai fini del presente articolo, l'espressione "informazioni relative agli abbonati" designa ogni informazione detenuta in forma di dato informatico o sotto altra forma da un fornitore di servizi e relativa agli abbonati ad un proprio servizio e diversa dai dati relativi al traffico o al contenuto e attraverso la quale è possibile stabilire:

a. il tipo di servizio di comunicazione utilizzato, le disposizioni tecniche prese a tale riguardo e il periodo del servizio;

b. l'identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento, disponibili sulla base degli accordi o del contratto di fornitura del servizio;

c. ogni altra informazione sul luogo di installazione dell'apparecchiatura della comunicazione, disponibile sulla base degli accordi o del contratto di fornitura del servizio.

TITOLO IV
PERQUISIZIONE E SEQUESTRO DI DATI INFORMATICI IMMAGAZZINATI

Articolo 19
Perquisizione e sequestro dati informatici immagazzinati

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di perquisire o accedere in modo simile:

a. a un sistema informatico o parte di esso e ai dati informatici ivi immagazzinati; e

b. a supporto per la conservazione di dati informatici nel quale i dati stessi possono essere immagazzinati nel proprio territorio.

2. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire che, qualora le proprie autorità perquisiscano o accedano in modo simile a specifici sistemi informatici o parte di essi, in conformità al paragrafo 1.a, e abbiano ragione di ritenere che i dati ricercati si trovino presso un altro sistema informatico o parte di esso nel proprio territorio, e a tali dati sia possibile legalmente l'accesso dal sistema iniziale, le stesse autorità possano estendere rapidamente la perquisizione o l'accesso all'altro sistema.

3. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di sequestrare o acquisire in modo simile i dati informatici per i quali si è proceduto all'accesso in conformità ai paragrafi 1 o 2. Tali misure devono includere il potere di:

a. sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici;

b. fare e trattenere una copia di quei dati informatici ;

c. mantenere l'integrità dei relativi dati informatici immagazzinati;

d. rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato.

4. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di ordinare ad ogni soggetto che abbia conoscenza del funzionamento del sistema informatico o delle misure utilizzate per proteggere i dati informatici in esso contenuti, di mettere a disposizione tutte le informazioni ragionevolmente necessarie per consentire l'applicazione delle misure di cui ai paragrafi 1. e 2.

5. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

TITOLO V
RACCOLTA IN TEMPO REALE DI DATI INFORMATICI

Articolo 20
Raccolta in tempo reale di dati sul traffico

1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di:

a. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici nel suo territorio;

b. obbligare un fornitore di servizi, nell'ambito delle sue capacità tecniche a:

i. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel suo territorio, o

ii. cooperare ed assistere le autorità competenti nella raccolta o registrazione in tempo reale di dati sul traffico associati a comunicazioni specifiche effettuate sul proprio territorio attraverso un sistema informatico.

2. Qualora una Parte, a causa dei limiti previsti dal proprio ordinamento giuridico, non è in grado di applicare le misure previste al paragrafo 1.a, può, invece, adottare le misure legislative o di altra natura che dovessero essere necessarie per consentire la raccolta o la registrazione in tempo reale dei dati relativi al traffico associati a comunicazioni specifiche effettuate sul proprio territorio, attraverso l'utilizzo di strumenti tecnici esistenti su questo territorio.

3. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per obbligare un fornitore di servizi a mantenere segreti il fatto che un qualsiasi potere previsto nel presente articolo sia stato esercitato e ogni informazione relativa.

I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

Articolo 21
Intercettazione di dati relativi al contenuto

1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie, in relazione ad una serie di gravi infrazioni che devono essere definite dal diritto nazionale, per consentire alle proprie competenti autorità di:

a. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, e

b. obbligare un fornitori di servizi, nell'ambito delle sue capacità tecniche a:

i. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, o

II. cooperare ed assistere le autorità competenti nella raccolta o registrazione in tempo reale di dati relativi al contenuto di comunicazioni specifiche eseguite nel proprio territorio attraverso un sistema informatico.

2. Qualora una Parte, a causa dei principi del proprio ordinamento giuridico, non è in grado di applicare le misure previste al paragrafo 1.a, può invece adottare misure legislative e di altra natura che dovessero essere necessarie per assicurare la raccolta o la registrazione in tempo reale dei dati relativi al contenuto di comunicazioni specifiche eseguite sul proprio territorio, attraverso l'utilizzo di strumenti tecnici in quel territorio.

3. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per obbligare un fornitore di servizi a mantenere segreto il fatto che un qualsiasi potere previsto nel presente articolo sia stato sia stato esercitato e ogni informazione relativa.

4.I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

SEZIONE III
COMPETENZA

Articolo 22
Competenza

1.Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per stabilire la propria competenza per tutti i reati previsti in conformità agli articoli da 2 a 11 della presente Convenzione, quando i reati siano commessi:

a. nel proprio territorio;

b. a bordo di una nave battente bandiera della Parte;

c. a bordo di un aeromobile immatricolato presso quella Parte;

d. da un proprio cittadino, se l'infrazione è penalmente punibile la dove è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato.

2. Ogni Parte può riservarsi il diritto di non applicare o di applicare solo in condizioni o casi specifici le regole di competenza definite ai paragrafi 1.b - 1.d del presente articolo o in una parte qualunque di essi.

3. Ogni Parte deve adottare le misure che dovessero essere necessarie per stabilire la propria competenza in ordine alle infrazioni di cui all'articolo 24, paragrafo 1 della presente Convenzione, nel caso in cui l'autore presunto dell'infrazione si trovi nel proprio territorio e

non è estradabile verso un'altra Parte solo in virtù della sua nazionalità, dopo una richiesta di estradizione.

4. La presente Convenzione non esclude alcuna competenza penale esercitata da una Parte in base al proprio diritto interno.

5. Quando più di una Parte rivendica la propria competenza per una presunta infrazione prevista dalla presente Convenzione, le Parti coinvolte si consultano, laddove sia opportuno, al fine di stabilire la competenza più appropriata per esercitare l'azione penale.

CAPITOLO III
COOPERAZIONE INTERNAZIONALE

SEZIONE II
PRINCIPI GENERALI

TITOLO I
PRINCIPI GENERALI RELATIVI ALLA COOPERAZIONE INTERNAZIONALE

Articolo 23
Principi generali relativi alla cooperazione internazionale

Le parti devono cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti i reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato, in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione internazionale in materia penale, degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale.

TITOLO II
PRINCIPI RELATIVI ALL'ESTRADIZIONE

Articolo 24
Estradizione

1. a. Il presente articolo si applica all'estradizione tra Parti per i reati stabiliti in base agli articoli da 2 a 11 della presente Convenzione, a condizione che essi siano punibili in base

alla legge di entrambe le Parti con la privazione della libertà per un periodo massimo di almeno un anno, o con una pena più severa.

b. Qualora sia richiesta una pena minima differente in base ad un trattato di estradizione applicabile fra due o più parti, ivi compresa la Convenzione Europea d'Estradizione (STE No. 24) o in forza di un accordo stipulato sulla base di legislazioni uniformi o reciproche, si applica la pena minima prevista in base a questi trattati o accordi.

2. I reati descritti al paragrafo 1 del presente articolo devono essere considerati come inclusi nel novero dei reati che possono dar luogo ad estradizione in tutti i trattati di estradizione esistenti tra le Parti. Le Parti si impegnano ad includere tali reati fra quelli che possono comportare l'estradizione in ogni trattato di estradizione che sarà concluso tra di esse.

3. Qualora una Parte condizioni l'estradizione all'esistenza di un trattato e riceva una richiesta di estradizione di un'altra Parte con la quale non ha un trattato di estradizione, la presente Convenzione può essere considerata come base giuridica per l'estradizione nei riguardi di tutti i reati menzionati al paragrafo 1 del presente articolo.

4. Le Parti che non condizionano l'estradizione all'esistenza di un trattato devono considerare i reati menzionati al paragrafo 1 del presente articolo come reati che possono dar luogo ad estradizione tra di esse.

5. L'estradizione è soggetta alle condizioni previste dal diritto interno della Parte richiedente o dai trattati di estradizione in vigore, inclusi i motivi in base ai quali la Parte richiesta può rifiutare di concedere l'estradizione.

6. Qualora l'estradizione per un reato menzionata al paragrafo 1 del presente articolo venga rifiutata esclusivamente sulla base della nazionalità della persona ricercata, o perché la Parte richiesta eccepisce la propria competenza per quel reato, la Parte richiesta deve sottoporre il caso su richiesta della Parte richiedente alla proprie autorità competenti a procedere e dovrà trasmettere i risultati finali alla Parte richiedente in tempo utile. Tali autorità dovranno prendere le proprie decisioni e condurre le proprie indagini e i procedimenti allo stesso che per tutti gli altri reati comparabili per natura in base alla legislazione di tale Parte.

7. a. Ogni Parte, al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, deve comunicare al Segretariato Generale del Consiglio d'Europa il nome e l'indirizzo di ogni autorità responsabile dell'invio o della ricezione delle richieste di estradizione o di arresto provvisorio in mancanza di un trattato.

b. Il Segretariato Generale del Consiglio d'Europa deve istituire e aggiornare un registro delle autorità a tal fine designate dalle Parti. Ogni Parte deve assicurare che i dati del registro siano corretti in ogni momento.

TITOLO III
PRINCIPI GENERALI RELATIVI ALLA MUTUA ASSISTENZA

Articolo 25
Principi generali relativi alla mutua assistenza

1. Le Parti devono concedersi reciprocamente la più ampia mutua assistenza al fine delle indagini o dei procedimenti relativi ai reati relativi a sistemi e dati informatici o per la raccolta di prove in formato elettronico di reati.
2. Ogni Parte deve anche adottare le misure legislative ed di altra natura che dovessero essere necessarie per l'adempimento degli obblighi assunti in base agli articoli da 27 al 35.
3. Ogni Parte può, in casi d'urgenza, fare richieste di mutua assistenza o comunicazioni ad essa relative attraverso strumenti rapidi di comunicazione, come il fax o la posta elettronica, a condizione che tali strumenti diano appropriate garanzie di sicurezza e autenticazione (inclusa la criptazione, se necessaria), seguite da conferma ufficiale ulteriore se lo Stato richiesto lo esige. Lo Stato richiesto deve accettare la domanda e rispondere alla richiesta con uno qualsiasi di tali mezzi rapidi di comunicazione.
4. Salva contraria disposizione espressamente prevista negli articoli del presente capitolo, la mutua assistenza è soggetta alle condizioni previste dalla legislazione della Parte richiesta o dai trattati di mutua assistenza applicabili, inclusi i motivi sulla base dei quali la Parte richiesta può rifiutare la cooperazione. La Parte richiesta non può esercitare il diritto di rifiutare la mutua assistenza in relazione ai reati menzionati negli articoli da 2 a 11 per il solo motivo che la richiesta riguarda un reato che essa reputa di natura fiscale.
5. Qualora, in conformità alle previsioni del presente capitolo, la Parte richiesta è autorizzata a subordinare la mutua assistenza ad una doppia incriminazione, questa condizione sarà considerata come soddisfatta, se il comportamento considerato reato per il quale la mutua assistenza è stata richiesta costituisca reato in base al proprio diritto interno, a prescindere dal fatto che la propria legislazione classifichi o meno il reato nella stessa categoria o lo denomini con la stessa terminologia della legislazione della Parte richiedente.

Articolo 26
Informazioni spontanee

1. Una Parte può, nei limiti della propria legislazione nazionale e senza una richiesta preventiva, trasmettere ad un'altra Parte informazioni ottenute nell'ambito delle proprie indagini qualora ritenga che la comunicazione di tali informazioni possa aiutare la Parte ricevente nell'avvio o nello svolgimento di indagini o procedimenti riguardanti reati definiti in

base alla presente Convenzione o possa giovare ad una richiesta di quella Parte in base al presente capitolo.

2. Prima di trasmettere tali informazioni, la Parte trasmittente può richiedere che esse vengano mantenute confidenziali o usate solo a determinate condizioni. Qualora la Parte ricevente non possa adeguarsi a tale richiesta, essa deve informare l'altra Parte, che dovrà quindi stabilire se le informazioni debbano comunque essere trasmesse. Qualora la Parte ricevente accetti le informazioni alle condizioni stabilite, essa dovrà attenervisi.

TITOLO IV
PROCEDURE RELATIVE ALLE RICHIESTE DI MUTUA ASSISTENZA IN ASSENZA DI ACCORDI INTERNAZIONALI APPLICABILI

Articolo 27
Procedure relative alle richieste di mutua assistenza in assenza di accordi internazionali applicabili

1. Qualora non vi sia un trattato o un accordo di mutua assistenza concluso sulla base di una legislazione uniforme in vigore o in condizione di reciprocità tra la Parte richiedente e richiesta, si applicano le disposizioni dei paragrafi da 2 a 9 del presente articolo. Le stesse non si applicano qualora vi sia un trattato, accordo o legislazione in vigore, a meno che le Parti interessate siano d'accordo nell'applicare a loro posto in tutto o in parte questo articolo.

2. a. Ogni Parte deve designare un'autorità centrale responsabile dell'invio e delle risposte alle richieste di mutua assistenza, dell'esecuzione di tali richieste o della loro trasmissione alle autorità competenti per la loro esecuzione.

b. Le autorità centrali devono comunicare direttamente tra loro;

c. Ogni Parte, al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, deve comunicare al Segretariato Generale del Consiglio d'Europa il nome e l'indirizzo dell'autorità designata in applicazione del presente paragrafo;

d. Il Segretariato Generale del Consiglio d'Europa deve istituire e tenere aggiornato un registro delle autorità centrali designate dalle Parti. Ogni Parte deve assicurare che i dati del registro siano corretti in ogni momento.

3. Le domande di mutua assistenza avanzate in base al presente articolo devono essere eseguite in conformità alle procedure specificate dalla Parte richiedente, salvo che siano incompatibili con la legislazione della Parte richiesta.

4. La Parte richiesta può, in aggiunta ai motivi di rifiuto stabiliti dall'articolo 25, paragrafo 4, rifiutare l'assistenza se:

a. la richiesta riguarda un reato che la Parte richiesta considera politico o connesso con un reato politico, o

b. la Parte richiesta ritenga che l'esecuzione della richiesta possa recare pregiudizio alla propria sovranità, alla sua sicurezza, all'ordine pubblico o ad altri interessi essenziali.

5. La Parte richiesta può sospendere l'esecuzione di una richiesta se la stessa può pregiudicare indagini o procedimenti condotti dalle proprie autorità.

6. Prima di rifiutare o sospendere l'assistenza, la Parte richiesta deve, se del caso dopo essersi consultata con la Parte richiedente, considerare se la richiesta possa essere eseguita in parte o sottoposta alle condizioni che ritenga necessarie.

7. La Parte richiesta deve prontamente informare la Parte richiedente del seguito che intende dare alla richiesta di assistenza. Essa dovrà motivare ogni rifiuto o sospensione della richiesta. La Parte richiesta deve anche informare la Parte richiedente di tutte le motivazioni che rendono impossibile l'esecuzione della richiesta o che sono in grado di ritardarla in modo significativo.

8. La Parte richiedente può richiedere che la Parte richiesta mantenga confidenziale il fatto e anche l'oggetto di ogni richiesta fatta in base al presente capitolo, salvo nella misura in cui sia necessario per la sua esecuzione. Qualora la Parte richiesta non possa adeguarsi la richiesta di confidenzialità, essa deve prontamente informare l'altra Parte, che dovrà quindi stabilire se la richiesta debba comunque essere eseguita.

9. a. In caso di urgenza, le richieste di mutua assistenza o le comunicazione ad essa collegate possono essere trasmesse direttamente alle autorità giudiziarie della Parte richiedente dalle autorità della Parte richiesta. In tale caso, una copia deve essere trasmessa contemporaneamente all'autorità centrale della Parte richiesta attraverso l'autorità centrale della Parte richiedente.

b. Ogni richiesta o comunicazione in base al presente paragrafo può essere effettuata attraverso l'Organizzazione Internazionale della Polizia Criminale (Interpol).

c. Qualora una richiesta venga effettuata in base al punto a. del presente articolo e l'autorità non sia competente ad esaminarla, essa deve trasmetterla all'autorità nazionale competente ed informarne direttamente la Parte richiedente.

d. Le richieste o le comunicazioni effettuate in base a questo paragrafo che non implichino azioni coercitive possono essere direttamente trasmesse dalle autorità competenti della Parte richiedente alle autorità competenti della Parte richiesta.

e. Ogni Parte può, al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, comunicare al Segretariato Generale del

Consiglio d'Europa che, per ragioni di efficienza, le richieste effettuate in base al presente paragrafo dovranno essere indirizziate alla propria autorità centrale.

Articolo 28
Confidenzialità e limitazioni di utilizzo

1. Quando non vi è un trattato o un accordo di mutua assistenza sulla base di una legislazione uniforme o in condizione di reciprocità in vigore tra la Parte richiedente e la Parte richiesta, devono applicarsi le disposizioni del presente articolo. Le disposizioni del presente articolo non si applicano qualora vi sia un trattato, accordo o legislazione in vigore, a meno che le Parti interessate siano d'accordo nell'applicare a loro posto in tutto o in parte il presente articolo.
2. La Parte richiesta può subordinare la comunicazione di informazioni o materiali in risposta ad una richiesta alla condizione che :
   a. vengano mantenute confidenziali qualora la richiesta di mutua assistenza legale non possa essere soddisfatta in mancanza di tale condizione; o
   b. non vengano utilizzate per indagini o procedimenti diversi da quelli indicati nella richiesta.
3. Qualora la Parte richiedente non possa soddisfare una delle condizioni contenute nel paragrafo 2, essa deve prontamente informare l'altra Parte, che deve stabilire se l'informazione possa comunque essere trasmessa. Quando la Parte richiedente accetta la condizione, essa vi si dovrà attenere.
4. Ogni Parte che fornisca un'informazione o del materiale soggetto ad una condizione in base al paragrafo 2 può richiedere all'altra Parte precisazioni, in relazione a tale condizione, circa l'uso fatto di tale informazione o materiale.

SEZIONE II
DISPOSIZIONI SPECIFICHE

TITOLO I
MUTUA ASSISTENZA RELATIVA A MISURE PROVVISORIE

Articolo 29
Conservazione rapida di dati informatici immagazzinati

1. Una Parte può richiedere ad un'altra Parte di ordinare od ottenere in altro modo la conservazione rapida di dati immagazzinati attraverso un sistema informatico, situato nel

territorio di quest'altra Parte e nei confronti della quale la Parte richiedente intende avanzare una richiesta di mutua assistenza per la perquisizione o altro simile mezzo di accesso, per il sequestro o altro strumento simile, o per la divulgazione dei dati.

2. Una richiesta di conservazione effettuata in base al paragrafo 1 deve specificare:

a. l'autorità che richiede la conservazione;

b. il reato che costituisce oggetto di indagine e una breve esposizione dei fatti relativi;

c. i dati informatici immagazzinati da conservare e il loro legame con il reato;

d. tutte le informazioni utili ad identificare il custode dei dati informatici immagazzinati o il luogo dove si trova il sistema informatico;

e. la necessità della conservazione; e

f. che la Parte intende avanzare una richiesta di mutua assistenza per la perquisizione o altro simile mezzo di accesso, per il sequestro o uno strumento similare, o per la divulgazione dei dati.

3. Dopo aver ricevuto la richiesta da un'altra Parte, la Parte richiesta deve prendere tutte le misure appropriate per conservare rapidamente i dati specificati in base alla propria legge nazionale. Per rispondere ad una tale richiesta, la doppia incriminazione non è richiesta come condizione per provvedere alla conservazione.

4. Una Parte che richiede la doppia incriminazione come condizione di procedibilità per rispondere ad una richiesta di mutua assistenza per la perquisizione o altro simile mezzo di accesso, per il sequestro o altro strumento similare, o per la divulgazione dei dati immagazzinati può, riguardo a reati diversi da quelli definiti in base agli articoli da 2 a 11 della presente Convenzione, riservarsi il diritto di rifiutare la richiesta di conservazione in base al presente articolo, nei casi in cui ha ragione di ritenere che, al momento della divulgazione, la condizione della doppia incriminazione non possa realizzarsi.

5. Inoltre, una richiesta di conservazione può essere rifiutata solo se:

a. la richiesta è relativa ad un reato che la Parte richiesta considera un reato politico o un reato connesso ad un reato politico; o

b. la Parte richiesta ritenga che l'esecuzione della richiesta possa recare pregiudizio alla propria sovranità, alla sua sicurezza, all'ordine pubblico o ad altri interessi essenziali.

6. Qualora la Parte richiesta ritenga che la conservazione non assicurerà la disponibilità in futuro dei dati o comprometterà la confidenzialità o pregiudicherà in altro modo le indagini della Parte richiedente, essa deve prontamente informare la Parte richiedente che dovrà decidere se la richiesta vada comunque eseguita.

7. Tutte le conservazioni effettuate a seguito di una richiesta di cui al paragrafo 1 devono essere disponibili per un periodo non inferiore a sessanta giorni, al fine di permettere alla Parte richiedente di effettuare una richiesta per la perquisizione o altro simile mezzo di accesso, per il sequestro o altro strumento analogo, o per la divulgazione dei dati. A seguito

del ricevimento di tale richiesta, i dati dovranno continuare ad essere conservati in attesa della decisione su tale richiesta

Articolo 30

Divulgazione rapida di dati di traffico conservati

1. Qualora, nel corso dell'esecuzione di una richiesta effettuata sulla base dell'articolo 29 per conservare dati sul traffico relativi ad una specifica comunicazione, la Parte richiesta scopra che un *service provider* di un altro Stato sia coinvolto nella trasmissione della comunicazione, la Parte richiesta deve rapidamente trasmettere alla Parte richiedente una quantità sufficiente di dati concernenti il traffico che consenta di identificare il *service provider* e la via attraverso la quale la comunicazione fu effettuata.

2. La divulgazione di dati di traffico di cui al paragrafo 1 può essere rifiutata solo se:

a. la richiesta riguarda un reato che la Parte richiesta consideri un reato politico o un reato connesso ad un reato politico; o

b. la Parte richiesta ritenga che l'esecuzione della richiesta possa recare pregiudizio alla propria sovranità, alla sua sicurezza, al proprio ordine pubblico o ad altri interessi essenziali.

TITOLO II

MUTUA ASSISTENZA RELATIVA AI POTERI D'INDAGINE

Articolo 31

Mutua assistenza concernente l'accesso a dati informatici immagazzinati

1. Una Parte può richiedere ad un'altra Parte la perquisizione o altro simile mezzo di accesso, il sequestro o altro strumento simile, o la divulgazione dei dati immagazzinati attraverso un sistema informatico situato nel territorio della Parte richiesta, inclusi i dati che sono stati conservati in base all'articolo 29.

2. La Parte richiesta soddisfa la richiesta attraverso gli strumenti internazionali, gli accordi e le legislazioni alle quali si fa riferimento all'articolo 23, e conformandosi alle disposizioni del presente capitolo.

3. La richiesta deve essere soddisfatta al più presto possibile quando:

a. vi è motivo di ritenere che i dati relativi siano particolarmente a rischio di perdita o modificazioni; o

b. gli strumenti, gli accordi e le legislazione di cui al paragrafo 2 prevedano una cooperazione rapida.

Articolo 32

Accesso transfrontaliero a dati informatici immagazzinati con il consenso o quando pubblicamente disponibili

Una Parte può, senza l'autorizzazione di un'altra Parte:

a. accedere ai dati informatici immagazzinati disponibili al pubblico (fonti aperte), senza avere riguardo al luogo geografico in cui si trovano tali dati; o

b. accedere o ricevere, attraverso un sistema informatico nel proprio territorio, dati informatici immagazzinati situati in un altro Stato, se la Parte ottiene il consenso legale e volontario della persona legalmente autorizzata a divulgare i dati allo Stato attraverso tale sistema informatico.

Articolo 33

Mutua assistenza nella raccolta in tempo reale di dati sul traffico

1. Le Parti devono fornire mutua assistenza tra loro nella raccolta in tempo reale di dati sul traffico, associati a specifiche comunicazioni nel proprio territorio, trasmessi attraverso l'uso di un sistema informatico. Questa assistenza, soggetta alle disposizioni del paragrafo 2, è regolata dalle condizioni e dalle procedure previste dal diritto interno.

2. Tutte le Parti devono fornire questa assistenza almeno rispetto ai reati per i quali la raccolta in tempo reale dei dati sul traffico sarebbe possibile, in ambito interno, in una situazione analoga.

Articolo 34

Mutua assistenza in materia di intercettazione di dati relativi al contenuto

Le Parti devono fornirsi mutua assistenza nella raccolta o registrazione in tempo reale di dati relativi al contenuto di specificate comunicazioni trasmesse attraverso l'uso di un sistema informatico nella misura consentita dai trattati applicabili fra le stesse e dalle leggi interne.

TITOLO III

RETE 24/7

Articolo 35

Rete 24/7

1. Ogni Parte deve designare un punto di contatto disponibile 24 ore su 24 e 7 giorni su 7, per assicurare un'assistenza immediata per le indagini relative a reati connessi a sistemi e

dati informatici, o per la raccolta di prove in formato elettronico di un reato. Tale assistenza deve includere la facilitazione o, se il diritto interno e la prassi nazionale lo consentono, l'applicazione diretta delle seguenti misure:

a. apporto di consigli tecnici;

b. conservazione dei dati in base agli articoli 29 e 30;

c. raccolta di prove, trasmissione di informazioni di carattere giuridico e localizzazione dei sospetti.

2. a. Il punto di contatto di una Parte deve poter comunicare con il punto di contatto di un'altra Parte secondo una procedura accelerata.

b. Se il punto di contatto designato da una Parte non dipende dall'autorità della Parte o delle autorità responsabili per la mutua assistenza internazionale o per l'estradizione, il punto di contatto dovrà garantire di essere in grado di coordinarsi con quella o con queste secondo una procedura accelerata.

3. Ogni Parte farà in modo di disporre di personale formato ed equipaggiato al fine di facilitare le attività della rete.

CAPITOLO IV
DISPOSIZIONI FINALI

Articolo 36
Firma ed entrata in vigore

1. Questa Convenzione è aperta alla firma degli Stati membri del Consiglio d'Europa e degli Stati non membri che hanno partecipato alla sua elaborazione.

2. Questa Convenzione è soggetta a ratifica, accettazione o approvazione. Gli strumenti di ratifica, accettazione o approvazione devono essere depositati presso il Segretariato Generale del Consiglio d'Europa.

3. Questa Convenzione entrerà in vigore il primo giorno del mese successivo alla scadenza dei tre mesi successivi alla data in cui cinque Stati, compresi almeno tre Stati membri del Consiglio d'Europa, avranno espresso il loro consenso ad essere vincolati dalla Convenzione conformemente alle disposizioni dei paragrafi 1 e 2.

4. Nei confronti di ogni Stato firmatario che esprima successivamente il proprio consenso, la Convenzione entrerà in vigore il primo giorno successivo la scadenza dei tre mesi successivi la data in cui viene espresso il consenso in conformità alle disposizioni dei paragrafi 1 e 2.

Articolo 37

Adesione alla Convenzione

1. Dopo l'entrata in vigore della presente Convenzione, il Comitato dei Ministri del Consiglio d'Europa, dopo avere consultato gli Stati Contraenti e dopo averne ottenuto il consenso unanime, può invitare ogni Stato che non sia membro del Consiglio e che non abbia partecipato alla elaborazione della Convenzione ad aderirvi. La decisione può essere presa a maggioranza secondo la disposizione dell'articolo 20.d. dello Statuto del Consiglio d'Europa e con voto unanime dei rappresentanti degli Stati contraenti aventi titolo a sedere nel Comitato dei Ministri.

2. Nei confronti di tutti gli Stati che abbiano aderito alla Convenzione in base al paragrafo 1. di cui sopra, la Convenzione entrerà in vigore il primo giorno del mese successivo alla scadenza dei tre mesi successivi alla data di deposito dello strumento di adesione presso il Segretariato Generale del Consiglio d'Europa.

Articolo 38

Applicazione territoriale

1. Ogni Stato può, al momento della firma o quando depositi il proprio strumento di ratifica, accettazione, approvazione o adesione, specificare il territorio o i territori ai quali la Convenzione si applica.
2. Ogni Stato può, successivamente, attraverso una dichiarazione indirizzata al Segretariato Generale del Consiglio d'Europa, estendere l'applicazione della Convenzione ad ogni altro territorio specificato nella dichiarazione. Nell'ambito di tale territorio la Convenzione entrerà in vigore il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data di ricevimento della dichiarazione da parte del Segretariato Generale.
3. Ogni dichiarazione effettuata in base ai due precedenti paragrafi può, nell'ambito di ogni territorio specificato in tale dichiarazione, essere revocata attraverso una notifica indirizzata al Segretariato Generale del Consiglio d'Europa. La revoca avrà effetto dal primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data di ricevimento di tale notifica da parte del Segretariato Generale.

Articolo 39

Effetti della Convenzione

1. Lo scopo della presente Convenzione è quello di completare i trattati e gli accordi multilaterali e bilaterali applicabili esistenti tra le Parti, incluse le disposizioni:

- della Convenzione europea sull'estradizione, aperta alla firma a Parigi, il 13 dicembre 1957 (ETS n. 24);

- della Convenzione europea sulla mutua assistenza in campo penale, aperta alla firma a Strasburgo, il 20 aprile 1959 (ETS n. 30);
- del Protocollo addizionale della Convenzione europea sulla mutua assistenza in campo penale, aperto alla firma a Strasburgo, il 17 MARZO 1978 (ETS n. 99).

2. Qualora due o più Parti abbiano già concluso un accordo o un trattato sulla materia trattata dalla presente Convenzione o abbiano in altro modo regolato le proprie relazioni su tali materie, o dovessero farlo in futuro, esse avranno anche facoltà d'applicare tale accordo o trattato o regolare le loro relazioni di conseguenza, in luogo della presenta Convenzione. Tuttavia, qualora le Parti stabiliscano le loro relazioni relative alle materie trattate nella presente Convenzione in modo diverso, esse dovranno farlo in modo che non sia incompatibile con l'oggetto e i principi della Convenzione.

3. Niente della presente Convenzione riguarda altri diritti, restrizioni, obbligazioni e responsabilità di una Parte.

Articolo 40

Dichiarazioni

Attraverso una dichiarazione scritta indirizzata al Segretariato Generale del Consiglio d'Europa, ogni Stato può, al momento della firma o quando depositi il proprio strumento di ratifica, accettazione, approvazione o adesione, dichiarare che si riserva la facoltà di richiedere elementi ulteriori come disposto dagli articoli 2, 3, 6 paragrafo 1 (b), 7, 9, paragrafo 3 e 27, paragrafo 9 (e).

Articolo 41

Clausola federale

1. Uno Stato federale può riservarsi il diritto di onorare gli impegni assunti in base al capitolo II della presente Convenzione nella misura in cui siano compatibili con i principi fondamentali che regolano i rapporti tra il proprio governo centrale e gli Stati membri o altre entità territoriali simili, a condizione che esso sia in grado di cooperare in base al capitolo III.

2. Quando effettua una riserva in base al paragrafo 1., uno Stato federale non può applicare i termini di tale riserva per escludere o diminuire sostanzialmente i propri obblighi di cui al capitolo II. In ogni caso, esso deve dotarsi di mezzi estesi ed effettivi che permettano la messa in opera delle misure previste da detto capitolo.

3. Nei riguardi delle disposizioni di questa Convenzione la cui applicazione ricade sotto la competenza di ciascuno Stato membro o di altra entità territoriale simile, che in base al sistema costituzionale della federazione non sia obbligato a prendere misure legislative, il governo federale deve informare le autorità competenti di tali Stati delle suddette

disposizioni, esprimendo parere favorevole e incoraggiandolo ad assumere iniziative adeguate per darvi esecuzione.

Articolo 42

Riserve

Con una notifica scritta indirizzata al Segretariato Generale del Consiglio d'Europa, ogni Stato può, al momento della firma o quando depositi il proprio strumento di ratifica, accettazione, approvazione o adesione, dichiarare che si avvale della riserva o delle riserve di cui all'articolo 4, paragrafo 2, articolo 6, paragrafo 3, articolo 9, paragrafo 4, articolo 10, paragrafo 3, articolo 11, paragrafo 3, articolo 14, paragrafo 3, articolo 22, paragrafo 2, articolo 29, paragrafo 4 e articolo 41, paragrafo 1. Non sono ammissibili altre riserve.

Articolo 43

Status e cancellazione delle riserve

1. La Parte che abbia formulato una riserva in conformità all'articolo 42 può ritirarla in tutto in parte inviando una notifica al Segretariato Generale del Consiglio d'Europa. Tale ritiro avrà effetto dalla data di ricevimento di tale notifica da parte del Segretariato Generale. Qualora la notifica indichi che il ritiro avrà effetto da una data specifica in essa indicata e tale data è successiva alla data della notifica, il ritiro ha effetto in tale data.
2. La Parte che abbia fatto una riserva come stabilito all'articolo 42 può ritirarla, in tutto o in parte, non appena le circostanze lo permettano.
3. Il Segretariato Generale del Consiglio d'Europa può periodicamente domandare alle Parti che hanno fatto una o più riserve di cui all'articolo 42 le prospettive del ritiro di tali riserve.

Articolo 44

Emendamenti

1. Emendamenti alla presente Convenzione possono essere proposti da ogni Parte e devono essere comunicati dal Segretariato Generale del Consiglio d'Europa agli Stati membri del Consiglio d'Europa, agli Stati non membri che hanno partecipato alla sua elaborazione e ad ogni Stato che vi ha aderito o è stato invitato ad aderirvi in conformità alle disposizioni dell'articolo 37.
2. Ogni emendamento proposto da una Parte deve essere comunicato al Comitato Europeo per i Problemi Criminali (CDPC), che dovrà sottoporre al Comitato dei Ministri il proprio parere su tale proposta di emendamento.
3. Il Comitato dei Ministri deve esaminare l'emendamento proposto e l'avviso espresso dal Comitato Europeo per i Problemi Criminali (CDPC) e, a seguito di consultazione degli Stati non membri Parti della presente Convenzione, può adottare l'emendamento.

4. Il testo di ogni emendamento adottato dal Comitato dei Ministri in conformità al paragrafo 3. del presente articolo deve essere trasmesso alle Parti per accettazione.

5. Ogni emendamento adottato in conformità al paragrafo 3. del presente articolo entrerà in vigore il trentesimo giorno dopo che tutte le Parti hanno informato il Segretariato Generale della loro accettazione.

Articolo 45

Risoluzione dei contrasti

Il Comitato Europeo per i Problemi Criminali (CDPC) deve essere informato della interpretazione e dell'applicazione della presente Convenzione.

Nel caso di un contrasto tra le Parti sull'interpretazione o applicazione della presente Convenzione, le Parti stesse si adopereranno per trovare una soluzione attraverso negoziati o con ogni altro pacifico strumento a loro scelta, inclusa la sottoposizione del contrasto al Comitato Europeo per i Problemi Criminali, ad un tribunale arbitrale la cui decisione sarà vincolante per le Parti, o alla Corte Internazionale di Giustizia, come concordato dalle Parti coinvolte.

Articolo 46

Consultazione delle Parti

1. Le Parti devono, quando occorra, consultarsi periodicamente allo scopo di facilitare:

a. l'effettivo uso e l'esecuzione della presente Convenzione, inclusa l'individuazione di ogni problema in materia, così come gli effetti di ogni dichiarazione o riserva fatta riguardo alla presente Convenzione;

b. lo scambio di informazioni sugli sviluppi legislativi, politici o tecnologici riguardanti la criminalità informatica e la raccolta di prove in formato elettronico;

c. l'esame di eventuali integrazioni o emendamenti della Convenzione.

2. Il Comitato Europeo per i Problemi Criminali (CDPC) deve essere mantenuto periodicamente informato dei risultati delle consultazioni di cui al paragrafo 1.

3. Il Comitato Europeo per i Problemi Criminali (CDPC) deve, quando occorra, facilitare le consultazioni di cui al paragrafo 1. e prendere le misure necessarie per assistere le Parti nel loro sforzo di integrare o modificare la Convenzione. Non oltre un triennio dall'entrata in vigore della Convenzione, il Comitato Europeo per i Problemi Criminali (CDPC) deve, in cooperazione con le Parti, procedere ad un riesame di tutte le disposizioni della Convenzione e, se necessario, consigliare tutte le modifiche opportune.

4. Salvi i casi in cui vengano assunte dal Consiglio d'Europa, le spese affrontate per l'esecuzione delle disposizioni del paragrafo 1. devono essere sostenute dalle Parti nel modo da esse stabilito.

5. Le Parti devono essere assistite dal Segretariato del Consiglio d'Europa nell'esercizio delle loro funzioni in base al presente articolo.

Articolo 47

Denuncia

1. Tutte le Parti possono, in ogni momento, denunciare la presente Convenzione attraverso la notifica al Segretariato Generale del Consiglio d'Europa.

2. Tale denuncia produce effetto a partire dal primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data di ricevimento della notifica da parte del Segretariato Generale.

Articolo 48

Notificazione

Il Segretariato Generale del Consiglio d'Europa dovrà notificare ad ogni Stato membro del Consiglio d'Europa, agli Stati non membri che hanno partecipato nell'elaborazione della presente Convenzione e ad ogni Stato che vi ha aderito o è stato invitato ad aderirvi:

a. tutte le firme;

b. il deposito di tutti gli strumenti di ratifica, accettazione, approvazione o adesione;

c. ogni data di entrata in vigore della presente Convenzione in base agli articoli 36 e 37;

d. ogni dichiarazione fatta in base all'articolo 40 o ogni riserve fatte in conformità all'articolo 42;

e. ogni altro atto, notifica o comunicazione relativa alla presente Convenzione.

In fede i sottoscritti, debitamente autorizzati a tal fine, hanno firmato la presente Convenzione .

Fatta a Budapest, il 23 novembre 2001, in inglese e francese, entrambi i testi egualmente autentici, in unica copia che dovrà essere depositata negli archivi del Consiglio d'Europa. Il Segretariato Generale del Consiglio d'Europa dovrà trasmettere copia certificata ad ogni Stato membro del Consiglio d'Europa, agli Stati non membri che hanno partecipato all'elaborazione della presente Convenzione e ad ogni Stato invitato ad aderirvi.

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Strasbourg, 28.I.2003

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, signatory hereto;

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

Recalling that all human beings are born free and equal in dignity and rights;

Stressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments;

Convinced that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;

Considering that national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems;

Aware of the fact that propaganda to such acts is often subject to criminalisation in national legislation;

Having regard to the Convention on Cybercrime, which provides for modern and flexible means of international co-operation and convinced of the need to harmonise substantive law provisions concerning the fight against racist and xenophobic propaganda;

Aware that computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;

Recognising that freedom of expression constitutes one of the essential foundations of a democratic society, and is one of the basic conditions for its progress and for the development of every human being;

Concerned, however, by the risk of misuse or abuse of such computer systems to disseminate racist and xenophobic propaganda;

Mindful of the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;

Recognising that this Protocol is not intended to affect established principles relating to freedom of expression in national legal systems;

Taking into account the relevant international legal instruments in this field, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination, the existing Council of Europe conventions on co-operation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia;

Welcoming the recent developments which further advance international understanding and co-operation in combating cybercrime and racism and xenophobia;

Having 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 developments of the new technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as "the Convention"), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Article 2 – Definition

1 For the purposes of this Protocol:

"*racist and xenophobic material*" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

2 The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

Chapter II – Measures to be taken at national level

Article 3 – Dissemination of racist and xenophobic material through computer systems

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

distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2 A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3 Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 – Racist and xenophobic motivated threat

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

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult

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

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2 A Party may either:

A - require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or

B - reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 –Denial, gross minimisation, approval or justification of genocide or crimes against humanity

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

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2 A Party may either

A - require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

B - reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 7 – Aiding and abetting

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, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Chapter III – Relations between the Convention and this Protocol

Article 8 – Relations between the Convention and this Protocol

1 Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, *mutatis mutandis*, to this Protocol.

2 The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol.

Chapter IV – Final provisions

Article 9 – Expression of consent to be bound

1 This Protocol shall be open for signature by the States which have signed the Convention, which may express their consent to be bound by either:

A - signature without reservation as to ratification, acceptance or approval; or

B - subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2 A State may not sign this Protocol without reservation as to ratification, acceptance or approval, or deposit an instrument of ratification, acceptance or approval, unless it has already deposited or simultaneously deposits an instrument of ratification, acceptance or approval of the Convention.

3 The instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

Article 10 – Entry into force

1 This Protocol 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 have expressed their consent to be bound by the Protocol, in accordance with the provisions of Article 9.

2 In respect of any State which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of its signature without reservation as to ratification, acceptance or approval or deposit of its instrument of ratification, acceptance or approval.

Article 11 – Accession

1 After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

2 Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession which shall take effect on the first day of the month following the expiration of a period of three months after the date of its deposit.

Article 12 – Reservations and declarations

1 Reservations and declarations made by a Party to a provision of the Convention shall be applicable also to this Protocol, unless that Party declares otherwise at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession.

2 By a written notification addressed to the Secretary General of the Council of Europe, any Party 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 Articles 3, 5 and 6 of this Protocol. At the same time, a Party may avail itself, with respect to the provisions of this Protocol, of the reservation(s) provided for in Article 22, paragraph 2, and Article 41, paragraph 1, of the Convention, irrespective of the implementation made by that Party under the Convention. No other reservations may be made.

3 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 in Article 5, paragraph 2.a, and Article 6, paragraph 2.a, of this Protocol.

Article 13 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 12 above shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. 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 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations in accordance with Article 12 as to the prospects for withdrawing such reservation(s).

Article 14 – Territorial application

1 Any Party 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 Protocol 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 Protocol to any other territory specified in the declaration. In respect of such territory, the Protocol 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 15 – Denunciation

1 Any Party may, at any time, denounce this Protocol 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 16 – 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 Protocol as well as any State which has acceded to, or has been invited to accede to, this Protocol 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 Protocol in accordance with its Articles 9, 10 and 11;

D - any other act, notification or communication relating to this Protocol.

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

Done at Strasbourg, this 28th day of January 2003, 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 Protocol, and to any State invited to accede to it.

CONSEIL DE L'EUROPE

Serie dei trattati europei - numero 189

Protocollo aggiuntivo alla Convenzione sulla Criminalità Informatica relativo alla criminalizzazione degli atti di natura razzista e xenofoba commessi attraverso i sistemi informatici

Strasburgo, 28.I.2003

Gli Stati membri del Consiglio d'Europa e gli altri Stati Parte alla Convenzione sulla Criminalità Informatica, aperta alla firma a Budapest il 23 novembre 2001, firmatari del presente Protocollo aggiuntivo;

Considerando che lo scopo del Consiglio d'Europa è di realizzare una maggiore unità tra i suoi membri;

Riconoscendo che tutti gli esseri umani nascono liberi ed eguali in dignità e diritti;

Sottolineando la necessità di garantire una piena ed efficace attuazione di tutti i diritti umani senza alcuna discriminazione o distinzione, come sancito negli strumenti europei e in altri strumenti internazionali;

Convinti che gli atti di natura razzista e xenofoba costituiscano una violazione dei diritti umani e una minaccia per lo stato di diritto e la stabilità democratica;

Ritenendo che il diritto nazionale e internazionale debba fornire adeguate risposte giuridiche alla propaganda di natura razzista e xenofoba effettuata per mezzo dei sistemi informatici;

Consapevoli del fatto che la propaganda di tali atti è spesso oggetto di criminalizzazione nella legislazione nazionale;

Vista la Convenzione sulla Criminalità Informatica, che prevede mezzi moderni e flessibili di cooperazione internazionale e convinti della necessità di armonizzare le disposizioni di diritto sostanziale riguardanti la lotta contro la propaganda razzista e xenofoba;

Consapevoli che i sistemi informatici offrono un mezzo senza precedenti volto a facilitare la libertà di espressione e di comunicazione in tutto il mondo;

Riconoscendo che la libertà di espressione costituisce uno dei fondamenti essenziali di una società democratica ed è una delle condizioni fondamentali per il suo progresso e per lo sviluppo di ogni essere umano;

Preoccupati, tuttavia, per il rischio di un utilizzo improprio o di abuso di tali sistemi informatici al fine di diffondere propaganda razzista e xenofoba;

Tenendo conto della necessità di garantire un giusto equilibrio tra la libertà di espressione e una lotta efficace contro gli atti di natura razzista e xenofoba;

Riconoscendo che il presente Protocollo non intende pregiudicare i principi della libertà di espressione negli ordinamenti giuridici nazionali;

Tenendo conto dei pertinenti strumenti giuridici internazionali in questo campo, e in particolare della Convenzione per la Salvaguardia dei Diritti Umani e delle Libertà Fondamentali e del suo Protocollo n. 12 concernente il divieto generale di discriminazione, le convenzioni esistenti del Consiglio d'Europa sulla cooperazione in campo penale, in particolare la Convenzione sulla Criminalità Informatica, la Convenzione Internazionale delle Nazioni Unite sull'Eliminazione di ogni Forma di Discriminazione Razziale del 21 dicembre 1965, l'Azione Comune dell'Unione Europea del 15 luglio 1996 adottata dal Consiglio sulla base dell'articolo K.3 del Trattato sull'Unione Europea, in materia di interventi di contrasto al razzismo e alla xenofobia;

Accogliendo positivamente i recenti sviluppi che favoriscono ulteriormente la comprensione e la cooperazione internazionali nella lotta contro la criminalità informatica e il razzismo e la xenofobia;

Visto il Piano di Azione adottato dai Capi di Stato e di Governo del Consiglio d'Europa in occasione del loro secondo vertice (Strasburgo, 10-11 ottobre 1997) per cercare risposte comuni rispetto agli sviluppi delle nuove tecnologie sulla base degli standard e dei valori del Consiglio d'Europa;

hanno convenuto quanto segue:

Capo I - Disposizioni comuni

Articolo 1 - Scopo

Lo scopo del presente Protocollo è di integrare, per ciò che concerne le Parti al presente Protocollo, le disposizioni della Convenzione sulla Criminalità Informatica, aperta alla firma a Budapest il 23 novembre 2001 (qui di seguito denominata "la Convenzione"), per quanto riguarda l'incriminazione di atti di natura razzista e xenofoba commessi attraverso i sistemi informatici.

Articolo 2 - Definizione

1 Ai fini del presente Protocollo si intende per:

"*materiale razzista e xenofobo*": qualsiasi materiale scritto, qualsiasi immagine o qualsiasi altra rappresentazione di idee o teorie che sostenga, promuova o inciti all'odio, alla discriminazione o alla violenza nei confronti di un individuo o di un gruppo di individui, sulla base della razza, del colore, dell'ascendenza o dell'origine nazionale o etnica nonché della religione, se addotti come pretesto per uno qualsiasi di questi fattori.

2 I termini e le espressioni utilizzati nel presente Protocollo sono interpretati nella stessa maniera in cui vengono interpretati ai sensi della Convenzione.

Capitolo II - Misure da adottare a livello nazionale

Articolo 3 - Diffusione di materiale razzista e xenofobo attraverso i sistemi informatici

1 Ciascuna Parte adotta le misure legislative e di altro tipo necessarie affinché le seguenti condotte siano considerate reati penali ai sensi del proprio diritto interno qualora compiute intenzionalmente e senza diritto:

distribuzione o qualsiasi altra forma di messa a disposizione al pubblico di materiale razzista e xenofobo attraverso un sistema informatico.

2 Una Parte può riservarsi il diritto di non prevedere la responsabilità penale per le condotte definite nel paragrafo 1 del presente articolo, nel caso in cui il materiale, come definito all'articolo 2, paragrafo 1, sostenga, promuova o inciti la discriminazione non associata all'odio o alla violenza, a condizione che siano disponibili altri rimedi efficaci.

3 In deroga al paragrafo 2 del presente articolo, una Parte può riservarsi il diritto di non applicare il paragrafo 1 a quei casi di discriminazione per i quali, a causa dei principi stabiliti nel proprio ordinamento giuridico nazionale in materia di libertà di espressione, non può fornire i rimedi efficaci di cui al precedente paragrafo 2.

Articolo 4 - Minaccia con motivazioni razziste e xenofobe

1 Ciascuna Parte adotta le misure legislative e di altro tipo necessarie affinché le seguenti condotte siano considerate reati penali ai sensi del proprio diritto interno qualora compiute intenzionalmente e senza diritto:

minacce, attraverso un sistema informatico, con la commissione di un grave reato penale come definito ai sensi del proprio diritto interno, (i) nei confronti di persone perché appartenenti a un gruppo identificato in base alla razza, al colore, all'ascendenza o all'origine nazionale o etnica, così come alla religione, se addotto come pretesto per uno qualsiasi di questi fattori, o (ii) nei confronti di un gruppo di persone identificato in base a una qualsiasi di queste caratteristiche.

Articolo 5 - Insulto con motivazioni razziste e xenofobe

1 Ciascuna Parte adotta le misure legislative e di altro tipo necessarie affinché le seguenti condotte siano considerate reati penali ai sensi del proprio diritto interno qualora compiute intenzionalmente e senza diritto:

insulto pubblico, attraverso un sistema informatico (i) di persone perché appartenenti a un gruppo identificato in base alla razza, al colore, all'ascendenza o all'origine nazionale o etnica, così come alla religione, se addotto come pretesto per uno qualsiasi di questi fattori, o (ii) di un gruppo di persone identificato in base a una qualsiasi di queste caratteristiche.

2 Una Parte può:

a richiedere che il reato di cui al paragrafo 1 del presente articolo abbia come effetto che la persona o il gruppo di persone di cui al paragrafo 1 sia esposto all'odio, al disprezzo o allo scherno; o

b riservarsi il diritto di non applicare, in tutto o in parte, il paragrafo 1 del presente articolo.

Articolo 6 – Negazione, minimizzazione grossolana, approvazione o giustificazione del genocidio o di crimini contro l'umanità

1 Ciascuna Parte adotta le misure legislative necessarie affinché le seguenti condotte siano considerate reati penali ai sensi del proprio diritto interno qualora compiute intenzionalmente e senza diritto:

la distribuzione o qualsiasi altra forma di messa a disposizione al pubblico, attraverso un sistema informatico, di materiale che neghi, minimizzi grossolanamente, approvi o giustifichi atti che costituiscono genocidio o crimini contro l'umanità, come definiti dal diritto internazionale e riconosciuti come tali dalle sentenze definitive e vincolanti del Tribunale Militare Internazionale, istituito con l'Accordo di Londra del 8 agosto 1945, o di qualsiasi altro tribunale internazionale istituito dai pertinenti strumenti internazionali e la cui giurisdizione è riconosciuta da detta Parte.

2 Una Parte può:

a richiedere che la negazione o la minimizzazione grossolana di cui al paragrafo 1 del presente articolo sia commessa con l'intento di incitare all'odio, alla discriminazione o alla violenza contro qualsiasi individuo o gruppo di individui, sulla base della razza, del colore, dell'ascendenza o dell'origine nazionale o etnica, così come della religione se addotti come pretesto per uno qualsiasi di questi fattori, o altrimenti

b riservarsi il diritto di non applicare, in tutto o in parte, il paragrafo 1 del presente articolo.

Articolo 7 - Favoreggiamento e complicità

Ciascuna Parte adotta le misure legislative e di altro tipo necessarie affinché venga considerato reato penale, ai sensi del proprio diritto interno, quando commesso intenzionalmente e senza diritto, il favoreggiamento o la complicità nella commissione di uno dei reati previsti dal presente Protocollo, con l'intenzione che sia commesso tale reato.

Capitolo III - Relazioni tra la Convenzione e il presente Protocollo

Articolo 8 - Relazioni tra la Convenzione e il presente

Protocollo

1 Gli articoli 1, 12, 13, 22, 41, 44, 45 e 46 della Convenzione si applicano, *mutatis mutandis*, al presente Protocollo.

2 Le Parti estendono il campo di applicazione delle misure definite agli articoli da 14 a 21 e agli articoli da 23 a 35 della Convenzione agli articoli da 2 a 7 del presente Protocollo.

Capitolo IV - Disposizioni finali

Articolo 9 - Espressione del consenso ad essere vincolati

1 Il presente Protocollo è aperto alla firma degli Stati che hanno firmato la Convenzione, che possono esprimere il loro consenso ad essere vincolati mediante:

a firma senza riserva di ratifica, accettazione o approvazione; oppure

b firma subordinata alla ratifica, all'accettazione o all'approvazione seguita dalla ratifica, accettazione o approvazione.

2 Uno Stato non può firmare il presente Protocollo senza riserve riguardo alla ratifica, all'accettazione o all'approvazione, né depositare uno strumento di ratifica, accettazione o approvazione, a meno che non abbia già depositato o non depositi contestualmente uno strumento di ratifica, accettazione o approvazione della Convenzione.

3 Gli strumenti di ratifica, accettazione o approvazione sono depositati presso il Segretario Generale del Consiglio d'Europa.

Articolo 10 - Entrata in vigore

1 Il presente Protocollo entra in vigore il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dopo la data in cui cinque Stati avranno espresso il loro consenso ad essere vincolati dal Protocollo, conformemente alle disposizioni dell'articolo 9.

2 Il Protocollo entra in vigore, per ogni Stato che esprime successivamente il suo consenso ad esserne vincolato, il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data di firma senza riserve per quanto riguarda la ratifica, l'accettazione o l'approvazione o di deposito dello strumento di ratifica, di accettazione o approvazione.

Articolo 11 - Adesione

1 Dopo l'entrata in vigore del presente Protocollo, qualsiasi Stato che abbia aderito alla Convenzione può aderire anche al Protocollo.

2 L'adesione avviene mediante il deposito presso il Segretario Generale del Consiglio d'Europa di uno strumento d' adesione che ha effetto il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data del suo deposito.

Articolo 12 - Riserve e dichiarazioni

1 Le riserve e le dichiarazioni formulate da una Parte relativamente a una disposizione della Convenzione si applicano anche al presente Protocollo, a meno che tale Parte dichiari diversamente al momento della firma o del deposito del proprio strumento di ratifica, accettazione, approvazione o adesione.

2 Con una notifica scritta indirizzata al Segretario Generale del Consiglio d'Europa, ciascuna Parte può, al momento della firma o del deposito del suo strumento di ratifica, accettazione, approvazione o adesione, dichiarare di avvalersi della o delle riserve previste agli articoli 3, 5 e 6 del presente Protocollo. Allo stesso tempo, una Parte può avvalersi, per quanto riguarda le disposizioni del presente Protocollo, della o delle riserve di cui all'articolo 22, paragrafo 2, e all'articolo 41, paragrafo 1, della Convenzione, indipendentemente dall'attuazione che ne fa detta Parte ai sensi della Convenzione. Nessuna altra riserva è ammessa.

3 Con una notifica scritta indirizzata al Segretario Generale del Consiglio d'Europa, ciascuna Parte può, al momento della firma o del deposito del suo strumento di ratifica, accettazione, approvazione o adesione, dichiarare di avvalersi della possibilità di richiedere ulteriori elementi previsti dall'articolo 5, paragrafo 2.a, e dall'articolo 6, paragrafo 2.a, del presente Protocollo.

Articolo 13 - Stato e ritiro delle riserve

1 Una Parte che ha formulato una riserva ai sensi del precedente articolo 12 ritira tale riserva, in tutto o in parte, non appena le circostanze lo consentano. Il ritiro ha effetto dalla data di ricevimento di una notifica indirizzata al Segretario Generale del Consiglio d'Europa. Se nella notifica si afferma che il ritiro di una riserva avrà effetto da un data ivi indicata, e tale data è successiva alla data in cui la notifica è stata ricevuta dal Segretario Generale, il ritiro ha effetto in tale data successiva.

2 Il Segretario Generale del Consiglio d'Europa può periodicamente richiedere alle Parti che hanno formulato una o più riserve a norma dell'articolo 12 informazioni in merito alle prospettive per il ritiro di tali riserve.

Articolo 14 - Applicazione territoriale

1 Ogni Parte può, all'atto della firma o del deposito del proprio strumento di ratifica, di accettazione, di approvazione o di adesione, designare il o i territori ai quali si applica il presente Protocollo.

2 Ogni Parte, in qualsiasi altro successivo momento, mediante una dichiarazione indirizzata al Segretario Generale del Consiglio d'Europa, può estendere l'applicazione del presente Protocollo ad ogni altro territorio designato nella dichiarazione. Il Protocollo entra in vigore nei confronti di detto territorio il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data di ricezione della dichiarazione da parte del Segretario Generale.

3 Ogni dichiarazione effettuata ai sensi dei due paragrafi precedenti può essere ritirata, per quanto concerne qualsiasi territorio designato in detta dichiarazione, per mezzo di una notifica indirizzata al Segretario Generale del Consiglio d'Europa. Il ritiro ha effetto il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data di ricezione della notifica da parte del Segretario Generale.

Articolo 15 - Denuncia

1 Ogni Parte può, in qualsiasi momento, denunciare il presente Protocollo indirizzando una notifica al Segretario Generale del Consiglio d'Europa.

2 Tale denuncia ha effetto il primo giorno del mese successivo allo scadere di un periodo di tre mesi dalla data di ricezione della notifica da parte del Segretario Generale.

Articolo 16 - Notifica

Il Segretario Generale del Consiglio d'Europa notifica agli Stati membri del Consiglio d'Europa, agli Stati non membri che hanno partecipato all'elaborazione del presente Protocollo, nonché ad ogni Stato che ha aderito o è stato invitato ad aderire al presente Protocollo, quanto segue:

a ogni firma;

b il deposito di ogni strumento di ratifica, accettazione, approvazione o adesione;

c ogni data di entrata in vigore del presente Protocollo conformemente alle disposizioni degli articoli 9, 10 e 11;

d ogni altro atto, notifica o comunicazione concernente il presente Protocollo.

In fede di ciò, il presente Protocollo è stato sottoscritto dai firmatari debitamente autorizzati.

Fatto a Strasburgo, il 28 gennaio 2003, in inglese e in francese, entrambi i testi facenti ugualmente fede, in un unico esemplare che è depositato negli archivi del Consiglio d'Europa. Il Segretario Generale del Consiglio d'Europa trasmette le copie certificate conformi a ciascuno Stato membro del Consiglio d'Europa, agli Stati non membri che hanno partecipato all'elaborazione del presente Protocollo, nonché ad ogni Stato invitato ad aderirvi.