Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version April 2008
[Reformat in March 2011]

Cybercrime legislation – country profile

ROMANIA

This profile has been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**Romania**
Signature of Convention:	23.11.2001
Ratification/accession:	12.05.2004
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": 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	**ART. 35 of Romania Law no 161/2003** (1) For the purpose of the present law, the terms and phrases below have the following meaning: a) *„computer system"* means any device or assembly of interconnected devices or that are in an operational relation, out of which one or more provide the

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	automatic data processing by means of a computer program; b) *„automatic data processing"* is the process by means of which the data in a computer system are processed by means of a computer program; c) *„computer program*" means a group of instructions that can be performed by a computer system in order to obtain a determined result; d) *„computer data"* are any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function; e) *„a service provider"* is: 1. any natural or legal person offering the users the possibility to communicate by means of a computer system; 2. any other natural or legal person processing or storing computer data for the persons mentioned in paragraph 1 and for the users of the services offered by these; f) *„traffic data"* are any computer data related to a communication by means of a computer system and generated by this, which represent a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication g*) "data on the users"* are represented by any information that can lead to identifying a user, including the type of communication and the serviced used, the post address, geographic address, IP address, telephone numbers or any other access numbers and the payment means for the respective service as well as any other data that can lead to identifying the user; h) *„security measures"* refers to the use of certain procedures, devices or specialised computer programs by means of which the access to a computer system is restricted or forbidden for certain categories of users; i) *„pornographic materials with minors"* refer to any material presenting a minor with an explicit sexual behaviour or an adult person presented as a minor with an explicit sexual behaviour or images which, although they do not present a real person, simulates, in a credible way, a minor with an explicit sexual behaviour. (2) For the purpose of this title, *a person acts without right* in the following situations: a) is not authorised, in terms of the law or a contract; b) exceeds the limits of the authorisation;

	c) has no permission from the competent natural or legal person to give it, according to the law, to use, administer or control a computer system or to carry out scientific research in a computer system. **General remark regarding the mental element.** Under the Romanian legal system ***an act that resides in an action committed with negligence shall be an offence only when the law provides this expressly*** (article 19 paragraphs 2 Criminal Code). As a result of this provision it was stated that there is no need to specify expressly the intentional element in the text. If the law **does not provide any mental element in the case of an offence consisting of an action the mental element required is intend**.
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.	**ART.42 of Romania Law no 161/2003** (1) The access without right to a computer system is a criminal offence and is punished with imprisonment from 6 months to 3 years or a fine. (2) Where the act provided in paragraph (1) is committed with the intent of obtaining computer data the punishment is imprisonment from 6 months to 5 years. (3) Where the act provided in paragraphs 1-2 is committed by infringing the security measures, the punishment is imprisonment from 3 to 12 years.
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.	**ART.43 of Romania Law no 161/2003** (1) The interception without right of non-public transmissions of computer data to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years. (2) The same punishment shall sanction the interception, without right, of electromagnetic emissions from a computer system carrying non-public computer data.

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.	**ART.44 of Romania Law no 161/2003** (1) The alteration, deletion or deterioration of computer data or restriction to such data without right is a criminal offence and is punished with imprisonment from 2 to 7 years. (2) The unauthorised data transfer from a computer system is punished with imprisonment from 3 to 12 years. (3) The same punishment as in paragraph (2) shall sanction the unauthorised data transfer by means of a computer data storage medium.
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	**ART.45 of Romania Law no 161/2003** The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data is a criminal offence and is punished with imprisonment from 3 to 15 years
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a	**ART.46 of Romania Law no 161/2003** (1) It is a criminal offence and shall be punished with imprisonment from 1 to 6 years. a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer program designed or adapted for the purpose of committing any of the offences established in accordance with Articles 42-45; b) the production, sale, import, distribution or making available, in any other form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of committing any of the offences established in accordance with Articles 42 - 45; 2) The same penalty shall sanction the possession, without right, of a device, computer program, password, access code or computer data referred to at paragraph (1) for the purpose of committing any of the offences established in accordance with Articles 42-45.

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.	**ART.48 of Romania Law no 161/2003** The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to such data, resulting in inauthentic data, with the intent to be used for legal purposes, is a criminal offence and shall be punished with imprisonment from 2 to 7 years.
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	**ART.49 of Romania Law no 161/2003** The causing of a loss of property to another person by inputting, altering or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another shall be punished with imprisonment from 3 to 12 years.

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.	**ART.51(1) of Romania Law no 161/2003** (1) It is a criminal offence and shall be punished with imprisonment from 3 to 12 years and denial of certain rights the production for the purpose of distribution, offering or making available, distributing or transmitting, procuring for oneself or another of child pornography material through a computer system, or possession, without right, child pornography material in a computer system or computer data storage medium.
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	**ART. 139[8] - 139 [9] and art. 143 of Law on copyright no.8/1996** **ART. 139^8** There is a criminal offence and shall be punished with imprisonment from 1 to

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.	4 years or a fine the act of making available to the public, including through the Internet or other computer networks, without the consent of the owners of the copyright of protected works, neighbouring rights or sui generis rights of the manufacturers of databases or copies of such protected work, regardless of the form of storage thereof, in such a manner as to allow to the public to access it from anywhere or at anytime individually chosen. **ART. 139^9** There is a criminal offence and shall be punished with imprisonment from 1 to 4 years or a fine the unauthorised reproduction in information systems of computer software in any of the following ways: install, storage, running or execution, display or intranet transmission. **ART. 143** (1) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of manufacturing, import, distribution or rental, offer, by any means, for sale or rental or possession in view of selling without right devices or components that allow neutralisation of technical measures of protection or that perform services that lead to neutralisation of technical measures of protection or that neutralise such technical measures of protection, including in the digital environment. (2) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of person whom, without having the consent of the owners of the copyright, and while knowing or should have known that thus is allowing, facilitating, causing or concealing a violation of a right as set forth in this law: a) removes or modifies from the protected works for commercial purposes any electronic information relating to the applicable regulations on copyright or neighbouring rights, b) distributes, imports in view of distribution, broadcasts or publicly communicates or makes available to the public, so as to allow access from any place and at any time chosen individually, without right, through digital technology, works or other protected works for which the information existing in electronic form regarding the regulations on copyright or related rights, have

	been removed or modified without authorisation.
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.	**For ART. 11 (1) of the Convention on Cybercrime – ART. 23, ART. 26, ART. 27 of Criminal Code** **Art.23 -** Persons who contribute to the commission of an act provided in the criminal law as authors, instigators or accomplices are participants. **Art.26 -** (1) An accomplice is a person who intentionally facilitates or helps in any way in the commission of an act provided in the criminal law. A person who promises, either before or during the commission of the offence, to conceal the proceeds emerging from it or to favour the perpetrator, even if after commission of the offence the promise is not kept, shall also be an accomplice. For ART. 11(2) of Convention on Cybercrime – ART. 47, ART.50 and ART. 51(2) of Romania Law no 161/2003 **Art.27** - Instigators and accomplices to an act provided in the criminal law committed with intent shall be sanctioned by the penalty provided in the law for authors. In establishing the penalty, each person's contribution to the commission of the offence, as well as Art. 72, shall be taken into account.

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.	**ART. 19[1] of Criminal Code (amended by Law no 278/2006)** **Article 12 – partially covered** Legal persons, with the exception of the State, the public authorities and the public institutions the activity of which is not the subject of private domain, shall be criminally liable for criminal offences committed in order to activate in their activity field or in the interest or on behalf of the legal person, provided that the act has been committed with the form of guilt provided in criminal law. Criminal liability of legal persons shall not exclude the criminal liability of natural persons who contributed in any manner to the perpetration of the same criminal 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.	**For art. 13(1) of Convention on Cybercrime - ART. 42-46, ART.48-49 and ART. 51 of Romania Law no 161/2003** **Art. 42** – (1) The access without right to a computer system is a criminal offence and is punished with imprisonment from 6 months to 3 years or a fine. (2) Where the act provided in paragraph (1) is committed with the intent of obtaining computer data the punishment is imprisonment from 6 months to 5 years. (3) Where the act provided in paragraphs 1-2 is committed by infringing the security measures, the punishment is imprisonment from 3 to 12 years. **Art. 43** – (1) The interception without right of non-public transmissions of computer data to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years. (2) The same punishment shall sanction the interception, without right, of electromagnetic emissions from a computer system carrying non-public computer data.

	Art. 44 – (1) The alteration, deletion or deterioration of computer data or restriction to such data without right is a criminal offence and is punished with imprisonment from 2 to 7 years. (2) The unauthorised data transfer from a computer system is punished with imprisonment from 3 to 12 years. (3) The same punishment as in paragraph (2) shall sanction the unauthorised data transfer by means of a computer data storage medium. **Art. 45** – The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data is a criminal offence and is punished with imprisonment from 3 to 15 years. **Art. 46** – (1) It is a criminal offence and shall be punished with imprisonment from 1 to 6 years. a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer program designed or adapted for the purpose of committing any of the offences established in accordance with Articles 42-45; b) the production, sale, import, distribution or making available, in any other form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of committing any of the offences established in accordance with Articles 42 - 45; 2) The same penalty shall sanction the possession, without right, of a device, computer program, password, access code or computer data referred to at paragraph (1) for the purpose of committing any of the offences established in accordance with Articles 42-45. **Art. 48** – The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to such data, resulting in inauthentic data, with the intent to be used for legal purposes, is a criminal offence and shall be punished with imprisonment from 2 to 7 years. **Art. 49** – The causing of a loss of property to another person by inputting, altering or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another shall be punished with

	imprisonment from 3 to 12 years. **Art.51** – (1) It is a criminal offence and shall be punished with imprisonment from 3 to 12 years and denial of certain rights the production for the purpose of distribution, offering or making available, distributing or transmitting, procuring for oneself or another of child pornography material through a computer system, or possession, without right, child pornography material in a computer system or computer data storage medium. (2) The attempt shall be punished. **For art. 13(2) of Convention on Cybercrime – ART. 53[1] of Criminal Code (amended by Law no 278/2006)** **ART. 53[1]** The penalties are: main and complementary. The main penalty is a fine from RON 2.500 to RON 2.000.000. Complementary penalties are: a) dissolution of the legal person; b) suspension of the activity of the legal person for a period from 3 months to one year or suspension of that of the activities of the legal person which served in the perpetration of the offence, for a period from 3 months to 3 years; c) closing of working locations belonging to the legal person, for a period from 3 months to 3 years; d) prohibition to participate in public procurement for a period from one to 3 years; e) display or broadcasting of the sentencing judgement.
Section 2 – Procedural law	
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;	**ART. 58 of Romania Law no 161/2003** The provisions of this chapter are applicable to criminal investigations or during the trial for the offences stipulated in this title or any other offences committed by means of computer systems.

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	**ART. 26 (1), 27 (3), 28 of Romania Constitution,** **Art.26 -** (1) An accomplice is a person who intentionally facilitates or helps in any way in the commission of an act provided in the criminal law. A person who promises, either before or during the commission of the offence, to conceal the proceeds emerging from it or to favour the perpetrator, even if after commission of the offence the promise is not kept, shall also be an accomplice. **Art.27** - Instigators and accomplices to an act provided in the criminal law committed with intent shall be sanctioned by the penalty provided in the law for authors. In establishing the penalty, each person's contribution to the commission of the offence, as well as Art. 72, shall be taken into account.

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.	**ART. 91[1] Criminal procedure Code, ART. 57 (1), (2) of Romania Law no 161/2003, ART. 3 (3), (5) of Romania Law no 365/2002 on electronic commerce (amended by Law no 121/2006)** **ART. 91[1] Criminal procedure Code** Legal persons, with the exception of the State, the public authorities and the public institutions the activity of which is not the subject of private domain, shall be criminally liable for criminal offences committed in order to activate in their activity field or in the interest or on behalf of the legal person, provided that the act has been committed with the form of guilt provided in criminal law. Criminal liability of legal persons shall not exclude the criminal liability of natural persons who contributed in any manner to the perpetration of the same criminal offence." **Art.57 of Romania Law no 161/2003 –** (1) The access to a computer system, as well as the interception or recording of communications carried out by means of computer systems are performed when useful to find the truth and the facts or identification of the doers cannot be achieved on the basis of other evidence. (2) The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed.
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	**ART.54 of Romania Law no 161/2003** (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered. (2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.

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.	(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days. (4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions. (5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used. (6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.
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.	**ART.54 of Romania Law no 161/2003** (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered. (2) During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order. (3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days. (4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve

	them under confidentiality conditions. (5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used. (6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.
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.	**ART. 16 of Law no 508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences** (2) The public prosecutors of the Directorate for Investigation of Offences of Organised Crime and Terrorism may ordain that they be communicated the originals or copies of any data, information, documents, banking, financial or accounting documents and other such items, by any person who holds them or from whom they emerge, and such person shall be bound to comply, under paragraph (1). (3) Failure to observe the obligation in paragraph (2) shall entail judicial liability, under the law.

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.	**For art. 19 (3) of Convention on Cybercrime –** **ART. 55 of Romanian Law 161/2003(in view of making copies that can serve as evidence);** (1) Within the term provided for at art. 54 paragraph (3), the prosecutor, on the basis of the motivated authorisation of the prosecutor specially assigned by the general prosecutor of the office related to the Court of Appeal or, as appropriate, by the general prosecutor of the office related to the Supreme Court, or the court orders on the seizing of the objects containing computer data, traffic data or data regarding the users, from the person or service provider possessing them, in view of making copies that can serve as evidence. (2) If the objects containing computer data referring to the data for the legal bodies in order to make copies, the prosecutor mentioned in paragraph (1) or court orders the forced seizure. During the trial, the forced seizure order is communicated to the prosecutor, who takes measures to fulfil it, through the criminal investigation body. (3) The copies mentioned in paragraph (1) are achieved by the technical means and the proper procedures to provide the integrity of the information contained by them. **ART. 96 and Art.99 of Criminal procedure Code.** **Art. 96 -** The criminal investigation body or the court must take away the objects or writings that may serve as means of evidence in the criminal trial. **Art. 99 –** If the object or writing required is not delivered voluntarily, the criminal investigation body or the court order confiscation by force. During the trial, the order of confiscation by force of objects or writings is communicated to the prosecutor, who takes enforcement measures through the criminal investigation body. **For art.19 (1-2) of Convention on Cybercrime - ART.56 (1) (3) of Romania Law no 161/2003.** (1) Whenever for the purpose of discovering or gathering evidence it is necessary to investigate a computer system or a computer data storage

	medium, the prosecutor or court can order a search. (3) When, on the occasion of investigating a computer system or a computer data storage medium it is found out that the computer data searched for are included on another computer system or another computer data storage medium and are accessible from the initial system or medium, it can be ordered immediately to authorize performing the search in order to investigate all the computer systems or computer data storage medium searched for.
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.	It is considered to be implemented by the new draft of the Criminal Procedure Code
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	**ART.57 of Romania Law no 161/2003** (1) The access to a computer system, as well as the interception or recording of communications carried out by means of computer systems are performed when

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.	useful to find the truth and the facts or identification of the doers cannot be achieved on the basis of other evidence. (2) The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed. (3) The authorisation referred to at paragraph (2) is given for 30 days at the most, with the extension possibility under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 4 months. (4) Until the end of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons against whom the measures referred to in paragraph (1) are taken. (5) The procedures of the Criminal procedure Code regarding the audio or video recordings are applied accordingly. **ART. 91[1] (Section V[1]) of the Criminal Procedure Code on audio and video interception and recording of conversations or communications by telephone or by any other electronic means of communication** **ART. 91[1] Criminal procedure Code** Legal persons, with the exception of the State, the public authorities and the public institutions the activity of which is not the subject of private domain, shall be criminally liable for criminal offences committed in order to activate in their activity field or in the interest or on behalf of the legal person, provided that the act has been committed with the form of guilt provided in criminal law. Criminal liability of legal persons shall not exclude the criminal liability of natural persons who contributed in any manner to the perpetration of the same criminal offence."
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be	**ART. 3-4 and art.142-143 Criminal Code**

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. 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.	**Art.3.** Criminal Law shall apply to offences committed on Romanian territory. **Art.4.** Criminal law shall apply to offences perpetrated outside the Romanian territory, if the perpetrator is a Romanian citizen or if he/she, while having no citizenship, domiciles in this country. **Art. 142.** The term "territory" in the phrases "Romanian territory" and "the territory of our country" means the surface of land and water that is comprised by the borders, with the subsoil and the aerial space, as well as the territorial sea with its soil, subsoil and aerial space. **Art. 143.** (1) "Offence committed on the territory of our country" means any offence committed on the territory shown in Art. 142 or on Romanian ships or aircraft. (2) An offence shall be deemed as committed on the territory of our country also when only an act of realisation was performed or only the result of the offence occurred on this territory or on Romanian ships or aircraft.
Chapter III – International co-operation	
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	**Art.23-24 (1) of Convention on cybercrime - ART.60 of Romania Law no 161/2003 and Title II of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006** (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain. (2) The cooperation, organised and carried out according to paragraph (1) can

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	have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.
Article 25 – General principles relating to mutual assistance	**ART.61 of Romania Law no 161/2003**

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.	(1) At the request of the Romanian competent authorities or of those of other states, on the territory of Romania common investigations can be performed for the prevention and fighting the cybercrime. (2) The common investigations referred to at paragraph (1) are carried out on the basis of bilateral or multilateral agreements concluded with the competent authorities. (3) The representatives of the Romanian competent authorities can participate in common investigations performed on the territory of other states by observing their legislation.
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	**ART.66 of Romania Law no 161/2003 and ART. 166 of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006**

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.	The competent Romanian authorities can send, ex-officio, to the competent foreign authorities, observing the legal provisions regarding the personal data protection, the information and data owned, necessary for the competent foreign authorities to discover the offences committed by means of a computer system or to solve the cases regarding these crimes.
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	**Single article (2) b) of Law no 64/2004 for ratification of the Council of Europe Convention on cybercrime**

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.	**ART. 12 of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006**
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	**ART.63 of Romania Law no 161/2003** (1) Within the international cooperation, the competent foreign authorities can require from the Service for combating cybercrime the expeditious preservation of the computer data or of the data regarding the traffic data existing within a computer system on the territory of Romania, related to which the foreign authority is to formulate a request of international legal assistance in criminal matters. (2) The request for expeditious preservation referred to at paragraph (1) includes the following: a) the authority requesting the preservation;

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. 4 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	b) a brief presentation of facts that are subject to the criminal investigation and their legal background; c) computer data required to be preserved; d) any available information, necessary for the identification of the owner of the computer data and the location of the computer system; e) the utility of the computer data and the necessity to preserve them; f) the intention of the foreign authority to formulate a request of international legal assistance in criminal matters; (3) The preservation request is executed according to art. 54 for a period of 60 days at the least and is valid until a decision is taken by the Romanian competent authorities, regarding the request of international legal assistance in criminal matters;

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.	**ART.64 of Romania Law no 161/2003** If, in executing the request formulated according to art.63 paragraph (1), a service provider in another state is found to be in possession of the data regarding the traffic data, the Service for combating cybercrime will immediately inform the requesting foreign authority about this, communicating also all the necessary information for the identification of the respective service provider.
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.	**ART. 60 of Romania Law no 161/2003** (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain. (2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.
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	**ART.65 of Romania Law no 161/2003** (1) A competent foreign authority can have access to public Romanian sources of computer data without requesting the Romanian authorities. (2) A competent foreign authority can have access and can receive, by means of a computer system located on its territory, computer data stored in Romania, if it has the approval of the authorised person, under the conditions of the law, to

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.	make them available by means of that computer system, without requesting the Romanian authorities.
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	**ART. 60 of Romania Law no 161/2003** (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain. (2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.
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.	**ART. 60 of Romania Law no 161/2003** (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain. (2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscation of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.
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	**ART. 62 of Romania Law no 161/2003** (1) In order to ensure an immediate and permanent international cooperation in the cybercrime area, within the Organised Crime Fighting and Anti-drug Section of the Prosecutor's Office belonging to the Supreme Court, a service for combating cybercrime is established as a contact point permanently available.

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.	(2) The Service for combating cybercrime has the following attributions: a) provides specialised assistance and information on Romanian legislation in the area to similar contact points in other states; b) orders the expeditious preservation of data as well as the seizure of the objects containing computer data or the data regarding the data traffic required by a competent foreign authority; c) executes or facilitates the execution, according to the law, of letters rogatory in cases of combating cybercrime cooperating with all the competent Romanian authorities.
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.	