www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Version July 2016

Cybercrime legislation – country profile

ROMANIA

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

Comments may be sent to:

Cybercrime Division
Directorate General of Human Rights and Rule of Law
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	Law No. 161/2003[1] (Title III - Prevention and combating cybercrime) implemented accurately the Budapest Convention. In 2004 Romania ratified the Convention on Cybercrime (Law no 64/2004). Subsequently, Romania had undertaken an ample legislative reform aimed at reviewing the entire criminal legislation. The process ended with the adoption of the new criminal and criminal procedure codes, as well as the laws enforcing them[2]. On 1 February 2014 they entered into force[3]. The new criminal codes incorporate the relevant substantive and procedural provisions related to cybercrime of the Law no 161/2003. Other relevant laws: ▪ Constitution of Romania ▪ Law no. 302/2004 on international judicial cooperation in criminal matters (amended and completed) ▪ Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (amended and completed) ▪ Law no. 8 of 14 March 1996 on copyright and neighbouring rights
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	**Article 35 of Law No. 161/2003** (1) In this title, the following words and expressions have the following meaning: a) **computer system** means any device or combination of interconnected devices or in a functional relation, one or more of which, pursuant to a program, performs

[1] Law No. 161/2003 on measures to ensure transparency in exercising public dignities, public functions and the business environment, preventing and sanctioning corruption, published in the Official Journal of Romania, Part I, No. 279 of 21 April 2003, with subsequent modifications and amendments

[2]
Law 286/2009 on the Criminal Code
Law 135/2010 on the new Criminal Procedure Code
Law 187/2012 enforcing the new Criminal Code
Law 255/2013 enforcing the new Criminal Procedure Code

[3] Available in English at: http://legislatie.just.ro/

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	automatic processing of data; b) **automatic data processing** means the process by which data from a computer system are processed through a computer program; c) **computer program** means a set of instructions that can be performed by a computer system to achieve a specific result; d) **computer data** means any representation of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can determine performance of a function by a computer system; e) **service provider** means: i. any natural or legal person that offers users the ability to communicate through computer systems; ii. any other natural or legal person that processes or stores data for the persons referred to under point 1 and for users of services provided by them; f) **data on traffic information** means any computer data related to a communication made via a computer system and its products, which is part of the communication chain, indicating the origin, destination, route, time, date, size, volume and duration, and type of service used for communication; g) **user data** means any information that may lead to the identification of a user, including type of communication and service used, address, geographical, phone numbers or any other access numbers and manner of payment of that service, and any other data that may lead to identification of the user; h) **security measures** mean the use of procedures, tools or specialized computer programs by which access to a computer system is restricted or prohibited for certain categories of users; **Criminal Code** **Art. 181 - Computer system and computer data** (1) Computer system means any device or combination of interconnected devices or in a functional relation, one or more of which, pursuant to a program, performs automatic processing of data; (2) Computer data mean any representation of facts, information or concepts in a form suitable for processing in a computer system. **Criminal Procedure Code**

	Art.138 (4) A **computer system** means any device or combination of interconnected devices or in a functional relation, one or more of which, pursuant to a program, performs automatic processing of data; (5) **Computer data** mean any representation of facts, information or concepts in a form appropriated for processing in a computer system, including a program able to determine the performance of a function by a computer system. ***Mental element*** **Law no 161/2003** (2) In the sense of this Title, the person in one of the following situations acts illegally: a) if he/she is not authorized by law or a contract; b) he/she exceeds the limits of authorisation; c) he/she does not have permission from the person or entity responsible, by law, to grant, use, manage or control a computer system or to conduct scientific research or perform any other operation in a computer system. **Criminal Code** **Art. 16 -Guilt** (1) An action only constitutes an offense if committed under the form of guilt required by criminal law. (2) Guilt exists when an action is committed with direct intent, with basic intent or oblique intent. (3) An action is committed with intent when the perpetrator: a) can foresee the outcome of their actions, in the expectation of causing such outcome by perpetrating the act; b) can foresee the outcome of their actions and, while not intending to produce it, nevertheless accepts the likelihood that it will occur. (4) An action is committed with basic intent when the perpetrator: a) can foresee the outcome of her/his action but does not accept it, believing without reason that such outcome will not occur; b) cannot foresee the outcome of her/his actions, though she/he should and could have done so. (5) Oblique intent exists when an act, consisting of an intentional action or inaction, causes unintended more serious consequences and is attributable to the perpetrator.

	(6) The act consisting of an action or inaction shall constitute an offense when committed with direct intent. The act committed with basic intent constitutes an offense only when the law expressly provides it. **Art. 17 - Perpetrated offense committed by omission** A perpetrated offense that requires causing a result is considered also committed by omission, when: a) there exists a legal or contract obligation to take action; b) the author of the omission, through previous action or inaction, created a state of threat for the protected social value, which facilitated the occurrence of the outcome.
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.	**Criminal Code** Title VII. Offenses against public security. Chapter VI- Offenses against security and integrity of computer systems and data **Art. 360 Illegal access to a computer system** (1) The access, without right, to a computer system shall be punished by imprisonment from 3 months to 3 years or a fine. (2) The act sets out in paragraph (1) committed in order to obtain computer data shall be punished by imprisonment from 6 months to 5 years. (3) If the act sets out in paragraph (1) was committed on a computer system to which, by procedures, devices or specialised programs, the access is restricted or prohibited for certain categories of users, the punishment is imprisonment from 2 to 7 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	**Criminal Code** **Art. 361 - Illegal interception of computer data transmissions** (1) The interception, without right, of a transmission of computer data, which is not public and is not intended for a computer system, originates from such computer system or is carried out within a computer system shall be punished with imprisonment from 1 to 5 years. (2) The same penalty shall apply to the interception, without right, of electromagnetic emissions from a computer system that contains computer data

connected to another computer system.	which is not public information.
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.	**Criminal Code** **Art. 362 - Altering computer data integrity** The act of altering, deleting or damaging computer data or restricting access to such data without right, shall be punished with imprisonment from 1 to 5 years. **Art. 364 – Unauthorised transfer of computer data** Unauthorised transfer of computer data from a computer system or a computer-data storage medium shall be punished with imprisonment from 1 to 5 years.
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	**Criminal Code** **Art. 363 - Disruption of the functioning of computer systems** The act of seriously disrupting, without right, the functioning of a computer system by inputting, transmitting, modifying, deleting or damaging data or by restricting the access to computer data shall be punished with imprisonment from 2 to 7 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 number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the	**Criminal Code** **Art. 365 Illegal operations with devices or computer programs** (1) Any person who, without right, produces, imports, distributes or makes available in any form: a) devices or computer programs designed or adapted for the purpose of perpetrating any of the offenses provided by art. 360 - 364; b) passwords, access codes or other such computer data that allow full or partial access to a computer system in order to perpetrate any of the offenses provided by art. 360-364 shall be punished with imprisonment from 6 months to 3 years or by a fine. (2) Possession, without right, of a device, computer program, password, access code or other computer data provided by paragraph (1) in order to perpetrate any of the offenses provided by art. 360-364 shall be punished with imprisonment from 3 months to 2 years or by a fine.

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.	**Criminal Code** Title VI. Offenses of forgery. Chapter III- Counterfeiting documents **Art. 325 - Computer data forgery** The input, alteration or deletion, without right, of computer data, or restricting, without right, the access to such data, resulting in inauthentic data, in order to be used for producing legal consequences, constitutes an offense and shall be punished with imprisonment from 1 to 5 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 benefit for oneself or for another person.	**Criminal Code** Title II. Offenses against property Chapter IV- Fraud perpetrated using computer systems and electronic payment methods **Art. 249 - Computer fraud** Entering, altering or deleting computer data, restricting the access to such data or preventing in any way the functioning of a computer system in order to obtain a benefit for oneself or for another, if it has caused damage to a person, shall be punished with imprisonment from 2 to 7 years.
Title 3 – Content-related offences	

Article 9 – Offences related to child pornography	**Criminal Code**
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 VIII. Offenses that harm relationships of social cohabitation Chapter I- Offenses against public order **Art. 374 - Child pornography** (1) The production, possession, procuring, storing, displaying, promotion, distribution or making available in any manner of child pornographic material shall be punished with imprisonment from 1 to 5 years. (1^1) With the penalty provided by paragraph (1) shall be punished inciting or recruiting of a minor to participate in a pornographic performance, obtaining benefits from such performance with minors or exploiting a minor in any other for carrying out pornographic performances. (1^2) Attending pornographic performances involving minors shall be punished with imprisonment from 3 months to 3 years or by a fine. (2) If the acts set out in paragraph (1) are perpetrated through a computer system or other mean of computer data storage the punishment is imprisonment from 2 to 7 years. (3) Accessing, without right, child pornographic material through computer systems or other means of electronic communication shall be punished with imprisonment from 3 months to 3 years or by a fine. (3^1) If the acts provided at paragraphs (1), (1^1), (1^2) and (2) have been perpetrated in the following circumstances: a) by a member of the family; b) by a person in which carrying, protection, education and surveillance or treatment the minor is or by a person having abused his/her position of trust or the authority over minor; c) the act put at risk the minor's life, the special limits shall be increased by one-half. (4) Child pornographic materials mean any material depicting a minor or a major presented as a minor having a sexually explicit behaviour or which, even if is not presenting a real person simulates a minor with such behaviour in a credible manner, as well as any depiction of a child's genital organs for sexual purpose. (5) The attempt shall be also punished. **Art. 35 of Law No. 161/2003** (1) In this title, the following words and expressions have the following meaning: i) child pornographic materials shall mean any material depicting a minor having an explicit sexual behavior or a major who is presented as a minor having an

	explicit sexual behavior or images which, although not representing a real person, simulates in a credible manner, a minor with an explicit sexual behavior.
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.	Law no. 8 of 14 March 1996 on copyright and neighboring rights, published in the Official Gazette of Romania no 60 of 26 March 1996 (subsequently amended and completed)
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	**Criminal Code** An **author** is the person who personally commits an act stipulated by criminal law

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.	(art. 46, paragraph (1), and co-authors are persons who personally commit the same act stipulated by criminal law (art. 46 paragraph 2). An **instigator** is a person who, with direct intent, determines another to commit an act stipulated by criminal law (Art. 47). The **accomplice** is the person who deliberately facilitates or helps in any way with the perpetration of an act stipulated by the criminal law (Art. 48 paragraph 1). The accomplice is also the person who promises, before or during the perpetration of the act, that he/she will conceal the goods originating from it or that he/she will favour the perpetrator, even if, after the perpetration of the act, the promise is not fulfilled (Art. 48 para. 2). The co-author, the instigator and the accomplice to a crime perpetrated with intent shall be punished with the penalty stipulated by law for the author. When the penalty is established, the contribution of each person to the commission of the act shall be taken into account, as well as the provisions provided by art. 74 (art. 49). In accordance with the provisions of the article 33 (1) **attempt** shall be punished only when the law expressly provides for. Consequently, attempt shall be punished in the case of the following offenses: Art. 249 (Computer fraud)[4], Art. 360 (Illegal access to a computer system)[5], Art. 361 (Illegal interception of computer data transmissions)[6], Art. 362 (Altering computer data integrity)[7], Art. 363 (Disruption of the operation of computer systems)[8], Art. 364 (Unauthorized transfer of computer data)[9], Art. 365 (Illegal operations with devices or software)[10], Art. 374 (Child pornography)[11].
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	**TITLE VI - Criminal Code** **Art. 135* - Conditions for the criminal liability of legal entities:** (1) Legal entity, except for state and public authorities, shall be held criminally

[4] Art. 252 of the Criminal Code
[5] Art. 366 of the Criminal Code
[6] Art. 366 of the Criminal Code
[7] Art. 366 of the Criminal Code
[8] Art. 366 of the Criminal Code
[9] Art. 366 of the Criminal Code
[10] Art. 366 of the Criminal Code
[11] Art. 374 (5) of the Criminal Code

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.	liable for offenses perpetrated in the performance of the object of activity of legal entities or in their interest or behalf. (2) Public institutions shall not be held criminally liable for offenses perpetrated in the performance of activities that cannot be the object of the private domain. (3) Criminal liability of legal entities does not exclude the criminal liability of the individual participating in the perpetration of the same act. *) Art. 240 of Law No. 187/2012 enforcing the new Criminal Code stipulates that, in the application of the provisions of Art. 135 of the Criminal Code, "public authorities" shall mean the authorities specifically referred to under Title III, as well as under Art. 140 and 142 of the Constitution of Romania, republished. **Art. 136 – The penalties applicable to legal entities** (1) The penalties applicable to legal entities include main penalties and complementary penalties. (2) The main penalty is fine. (3) The complementary penalties are: a) winding-up of legal entities; b) suspension of the activity or of one of the activities performed by the legal entity, for a term between three months and three years; c) closure of some working points of the legal entity for a term between three months and three years; d) prohibition to participate in public procurement procedures for a term between one and three years; e) placement under judicial supervision; f) display or publication of the conviction sentence.
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.	*See above the penalties.* The Criminal Code transposed Article 9 (Penalties) of the Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems, replacing Framework Decision 2005/222/JHA of the Council. ▪ Illegal access to a computer system – penalty up to 3 years imprisonment (art. 360) - if the act was committed in order to obtain computer data the penalty is up to 5 years imprisonment - art. 360 para.(2) - if the act was committed on a computer system to which, by procedures, devices or specialised programs, the access is restricted or prohibited for certain categories of users the penalty is up to 7 years imprisonment –

	art. 360 para.(3) ▪ Illegal interception of computer data transmissions: penalty up to 5 years imprisonment (art. 361) ▪ Altering computer data integrity: penalty up to 5 years imprisonment (art. 362) ▪ Disruption of the functioning of computer systems: penalty up to 7 years imprisonment (art. 363) ▪ Illegal operations with devices or computer programs: penalty up to 3 years imprisonment (art. 365) ▪ Computer data forgery: penalty up to 5 years imprisonment (art. 325) ▪ Computer data fraud: penalty is up to 7 years imprisonment (art. 249). ▪ Child pornography: penalty is up to 7 years imprisonment (art. 374). Of relevance also: ✓ Aggravating circumstances (Criminal Code, art. 77) ✓ Conjunction with organized crime offence (Criminal Code, art. 367) ✓ Aggravated computer fraud - Criminal code art.249 ref. to art. 256 [1]- a material damage exceeding 2,000,000 RON (Criminal Code, art. 183)
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; 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	***Electronic evidence*** Art. 97 of the Criminal Procedure Code provides that "*any factual element serving to the ascertaining of the existence or non-existence of an offense, to the identification of a person who committed such offense and to the knowledge of the circumstances necessary to a just settlement of a case, and which contribute to the finding of the truth in criminal proceedings represents evidence*". Thus, the evidence is obtained in criminal proceedings through means and objects of evidence and is presented through the methods of proof provided by law. Practice admits that the "electronic evidence" (digital evidence) represents *any factual element, created or existing in an electronic (digital) medium serving to the ascertaining of the existence or non-existence of an offense, to the identification of a person who committed such offense and to the knowledge of the circumstances necessary to a just settlement of a case.* Computer search is a method of proof, thus included in the processes for collecting evidence specific to criminal prosecution in case of cybercrime. It sets up the legal framework to obtain the means of proof making the electronic

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	evidence easy to understand by the human mind. With regard to production of evidence, including electronic evidence, the provisions of Article 100 of the Criminal Procedure Code provides that during the criminal investigation, investigation bodies gather and produce evidence both in favour and against a suspect or a defendant, ex officio or upon request, and, during the trial, this role belongs to the court, who produces evidence upon request by the prosecutor, the victim or the parties and, subsidiarily, ex officio, when it deems it necessary for the creation of its own conviction. The above-mentioned article establishes the main characteristics of the evidence, i.e. a piece of evidence should be relevant to the object of evidentiary in a case, as stipulated under Art. 98 of the Criminal Procedure Code. Also, the evidence must be necessary and useful, i.e. it is not meant to prove a fact of notoriety, or not sufficient evidence has been produced for proving a factual element representing the object of evidentiary, the piece of evidence is not impossible to obtain, the production of evidence is legal and was requested by a person who has such right. In making a decision the existence of an offense and on a defendant's guilt, the court decides, on a justified basis, on the basis of all the assessed pieces of evidence. Conviction is ordered only when the court is convinced that the charge was proven beyond any reasonable doubt. **Art.197 para.1 and 2** of the Criminal Procedure Code stipulates that objects containing or bearing traces of a committed offense are physical evidence (for example HDD, CD, DVD, router, memory stick or any other piece of equipment and the objects used to the commission of an offense are *corpus delicti* (for example the computer system used). Taking into account the particular nature of the evidence that is produced, transmitted or kept in a computer system, the Criminal Procedure Code has established special rules on how the electronic surveillance is performed, how computer search is carried out, and how computer data are surrendered or preserved. **Art. 142^1**: (1) Any authorized person conducting electronic surveillance activities, under this law, has the possibility to ensure the electronic signing of data resulting from electronic surveillance activities, by using an extended electronic signature based on a qualified certificate issued by an accredited certification services provider. (2) Any authorized person who transmits data resulting from electronic

	surveillance activities under this law, has the possibility to sign the transmitted data by using an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which allows for the unambiguous identification of the authorized person, the latter taking this way responsibility for the integrity of the transmitted data. (3) Any authorized person who receives data resulting from electronic surveillance activities under this law, has the possibility to check the integrity of the received data and to certify such integrity by signing them by means of an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which allows for the unambiguous identification of the authorized person. (4) Each person certifying data under electronic signature is liable for the security and integrity of such data under the law. The Criminal Procedure Code establishes under Chapter IV Art. 138 the **following special methods of surveillance or investigation:** a) wiretapping of communications or of any type of remote communication; b) accessing a computer system; c) video, audio or photo surveillance; d) tracking or tracing with the use of technical devices; e) obtaining data regarding the financial transactions of individuals; f) withholding, delivery or search of mail deliveries; g) use of undercover investigators and informants; h) authorized participation in specific activities; i) controlled delivery; j) obtaining traffic and location data processed by providers of public electronic communication networks or by providers of electronic communication services intended for the public. (2) Wiretapping of communications or of any type of messages means wiretapping, accessing, monitoring, collection or recording of communications via phone, computer system or any other communication device. (3) Accessing a computer system means penetration of a computer system or of other data storage device either directly or from the distance, through specialized programs or through a network, for the purpose of identifying evidence. […] (6) Video, audio or photo surveillance means taking of pictures of persons, observation or recording of their conversations, gestures or other activities. (7) Tracking or tracing with the use of technical devices means use of devices that

	establish the location of the person or the object to which such devices are attached. (8) Search of mail deliveries means inspection, through physical or technical methods, of letters or other mail deliveries or objects transmitted through any other means. (9) Obtaining of data regarding the financial transactions of individuals means operations that provide knowledge of the contents of financial transactions and other operations performed or to be performed through a credit institution or through other financial entity, as well as the obtaining from a credit institution or other financial entities of documents or information held by it referring to the transactions or operations of a person. (10) Use of undercover investigators and informants means use of a person with an identity other than their real one, for the purpose of obtaining data and information regarding the commission of an offense. (11) Authorized participation in specific activities means the commission of acts similar to the objective component of a corruption offense, the performance of transactions, operations or any other kind of arrangements related to an asset or to a person who is presumed missing, a victim of trafficking in human beings or of kidnapping, the performance of operations involving drugs, as well as the providing of services, based on an authorisation from the judicial bodies of competent jurisdiction for the purpose of obtaining evidence. (12) Controlled delivery designates a surveillance and investigation technique allowing for the entry, transit or exit from the territory of the country of goods in respect of which there is a suspicion related to the illicit nature of their possession or obtaining, under the surveillance of or based on an authorisation from the competent authorities, for the purpose of investigating an offense or of identifying the persons involved in its commission. (13) By electronic surveillance shall be understood the use of one of the methods foreseen in paragraphs (a) to (d). *Other measures:* ▪ Preservation of computer data (Art. 154) ▪ Computer search (Art. 168)
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	The Internet must be used with observance of the legal provisions, of the private life and fundamental rights. The communication via the Internet and other communication means is protected and guaranteed by the legal framework in

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.	force. At the same time, personal data are protected by the Romanian legislation in force, and illegal dissemination on the Internet of such data constitutes contravention and is sanctioned by a fine. Taking into account Romania's membership in the Council of Europe and in the European Union, the criminal reform in Romania aimed at adjusting the legislation in criminal matters to the exigencies and requirements of the European Convention for the Protection of Human Rights and Fundamental Freedoms, as well as of other relevant international and community instruments. The Constitution of Romania guarantees a series of fundamental human rights and freedoms, among which: Art. 26 - The intimate, family and private life Art. 27 - Inviolability of domicile Art. 28 - Secrecy of correspondence Art. 30 - Freedom of expression Art. 31 – The right to information etc. The above-mentioned constitutional principles are reflected in the criminal legislation, including the Criminal Procedure Code and the Criminal Code, through the incrimination of acts infringing upon the domicile and private life (Chapter IX, Special Part, "Crimes that harm private domicile and life"). The objectives of the new Criminal Procedure Code included the unitary protection of the human rights and freedoms guaranteed by the Constitution and by the international legal instruments, as well as the adequate regulation in the criminal legislation of the international obligations undertaken by Romania. In the same line of guaranteeing the right stipulated under Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Criminal Procedure Code establishes, as a principle, the obligation that, once the technical surveillance has ended, the prosecutor should inform in writing the subject of any warrant about the surveillance measure taken against them. Law No.677/2001 represents the legal framework on the protection of persons regarding the processing of personal data and the free movement of such data (published in the Official Journal No. 790 of 12 December 2001), the purpose of which is to guarantee and protect the rights and fundamental liberties of natural persons, especially the right to intimate, family and private life, in regard to processing personal data. According to Art. 53 from the Constitution of Romania, "(1)The exercise of certain

	rights or freedoms may only be restricted by law, and only if necessary, as the case may be, for: the defense of national security, of public order, health, or morals, of the citizens' rights and freedoms; conducting a criminal investigation; preventing the consequences of a natural calamity, disaster, or an extremely severe catastrophe. (2) Such restriction shall only be ordered if necessary in a democratic society. The measure shall be proportional to the situation having caused it, applied without discrimination, and without infringing on the existence of such right or freedom". In view of respecting the right to private life and correspondence, the Criminal Procedure Code establishes procedural rules concerning special methods of surveillance and investigation methods[12], which meet the criteria of accessibility, predictability and proportionality. In all cases of authorising these measures, the criminal law imposes that a reasonable suspicion should exist regarding the perpetration of a crime, that the principle of subsidiarity should be respected-being outlined the exceptional character of interference into one's private life- as well as the principle of the proportionality of the measure in regard to restricting the right to private life, related to the specificity of the case, the importance of the information or of the evidence that is to be obtained, or the seriousness of the crime. During a the criminal investigation, the Judge for Rights and Liberties of the court that would have the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office with which the prosecutor conducting or supervising the criminal investigation is working are located may order the conducting of a computer search, upon request by the prosecutor, when the investigation of a computer system or of a computer data storage medium is necessary for the discovery and collection of evidence. In respect to special methods of surveillance and the special investigation methods there are procedural distinctions, as well as substantive conditions related to the type of offense investigated. Thus electronic surveillance may be ordered only in case of offenses considered serious, listed under Art. 139 para.2. According to Art. 139 (1) Electronic surveillance is ordered by the Judge for Rights and Liberties when the following requirements are cumulatively met:

[12] Art.138 of the Criminal Procedure Code

	a) there is a reasonable suspicion in relation to the preparation or commission of one of the offenses listed under par. (2); b) such measure is proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offense; c) evidence could not be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat for the safety of persons or of valuable goods. (2) Electronic surveillance may be ordered in case of offenses against national security stipulated by the Criminal Code and by special laws, as well as in case of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism, money laundering, counterfeiting of currency or securities, counterfeiting electronic payment instruments, offenses against property, blackmail, rape, deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, offenses committed by means of computer systems or electronic communication devices, or in case of other offenses in respect of which the law sets forth a penalty of no less than 5 years of imprisonment. (3) The recordings set forth by this chapter, done by the parties or by other persons, represent evidence when they concern their own conversations or communications with third parties. Any other recordings may constitute evidence unless prohibited by law. (4) The relationship between a counsel and a person assisted or represented by them may be subject to electronic surveillance only when there is information that the counsel perpetrates or prepares the commission of any of the offenses listed under par.(2). If during or after the performance of such measure it results that the activities of electronic surveillance also targeted the relations between the counsel and the suspect or defendant defended by the former, the evidence obtained this way may not be used in a criminal proceeding, and shall be destroyed forthwith by the prosecutor. The judge having ordered such measure shall be informed forthwith by the prosecutor. When deemed necessary, the judge may order the information of the counsel. Pursuant to **Art.140 electronic surveillance** may be ordered during the criminal investigation, for a term of maximum 30 days, upon request by the prosecutor, the Judge for Rights and Liberties of the court having the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office

	to which the prosecutor who filed the application belongs are located. If they decide that the application is justified, the Judge for Rights and Liberties shall order admission of the prosecutor's application, through a court resolution, and shall issue forthwith an electronic surveillance warrant. Upon reasoned request by the victim, the prosecutor may request the judge to authorise wiretapping or recording of communications, as well as any type of communication performed by the person concerned via any means of communication, irrespective of the nature of the offense that is subject to investigation. Provisions of para. (1) - (8) apply accordingly. **Art. 141** provides for the situations in which the prosecutor may authorise for a period of maximum 48 hours, electronic surveillance measures, under the obligation to notify the Judge for Rights and Liberties within a maximum of 24 hours following expiry of a measure and forward a report presenting a summary of the electronic surveillance activities performed and the case file. In respect of computer data identified through accessing a computer system, the prosecutor may order, through a prosecutorial order: a) making and preservation of a copy of such computer data; b) prohibition of access to or removal of such computer data from the computer system. Copies shall be made by means of appropriate technical devices and procedures, of nature to ensure the integrity of information contained by these. The electronic surveillance warrant may be extended, for well-grounded reasons, by the Judge for Rights and Liberties of the court of competent jurisdiction, upon reasoned request by the prosecutor, in situations where certain requirements are met; however, each such extension may not exceed 30 days (Art. 144). Following the termination of an electronic surveillance measure, the prosecutor shall inform each subject of the warrant for electronic surveillance enforced against them, in writing, within maximum 10 days (Art. 145). Pursuant to Art. 147, withholding, surrender and search of postal deliveries may be ordered by the Judge for Rights and Liberties of the court on which would rest the competence of jurisdiction to settle the case in first instance or by the court having a corresponding level within the territorial jurisdiction of which falls the prosecutors' office to which the prosecutor having prepared the proposal belongs, in respect of letters, postal dispatches or items sent or received by a perpetrator, suspect, defendant or by any person suspected to receive or send, by any means, such goods from/to a perpetrator, suspect or defendant, or goods intended to it, if:

	a) there is a reasonable suspicion related to the preparation or commission of an offense; b) such step is necessary and proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or of evidence to be obtained or the offense seriousness; c) evidence could not be obtained in other way, or obtaining it would imply extreme difficulties that would harm the investigation or there is a threat against the safety of persons or of high value goods.
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.	**Criminal Procedure Code** **Preservation of computer data (Art. 154)** (1) If there is a reasonable suspicion in relation to the preparation or commission of an offense, for the purpose of collecting evidence or of identifying a perpetrator, suspect or defendant, the prosecutor supervising or conducting the criminal investigation may order immediate preservation of computer data, including of data referring to information traffic, that were stored by means of a computer system and that is in the possession or under the control of a provider of public electronic communication networks or of a provider of electronic communication services intended for the public, in the event that there is a danger that such data may be lost or altered. (2) The preservation is ordered by the prosecutor, ex officio or upon request by criminal investigation bodies, for a term of maximum 60 days, through an order that has to contain besides the obligations provided by Article 286 paragraph (2): the providers of public electronic communication networks or the providers of electronic communication services intended for the public in which possession or control the computer data is, the name of the perpetrator, suspect or defended if known, a description of the data to be preserved, justification of the fulfilment of the conditions required by paragraph 1, the duration for which it was issued, a mention of the obligation of the person or providers of public electronic communication networks or the providers of electronic communication services intended to immediately preserve the indicated computer data and maintain the data integrity, under conditions of confidentiality. (3) The preservation measure may be extended by the prosecutor, only once, for well-grounded reasons, for a term of maximum 30 days. (4) The prosecutor's order is transmitted immediately to any provider of public electronic communication networks or provider of electronic communication services intended for the public holding the data specified under paragraph (1) or

	having control on such data, the latter being under the obligation to preserve it immediately, under confidentiality terms. (5) If data referring to information traffic is held by several providers of public electronic communication networks or providers of electronic communication services intended for the public, a provider holding or controlling the computer data is under an obligation to provide the criminal investigation bodies forthwith with the information necessary for the identification of other providers, in order to enable them to learn of all elements of the used communication chain. (6) The prosecutor supervising or conducting the criminal investigation, based on a prior authorisation from the Judge for Rights and Liberties, may request a provider of public electronic communication networks or a provider of electronic communication services intended for the public to transmit the data preserved under the law or may order cancellation of such measure. (7) The Judge for Rights and Liberties shall rule on requests transmitted by criminal investigation bodies regarding the transmission of data within 48 hours, through a reasoned court resolution, in chambers. (7 [1]) Paragraphs (1) to (7) apply accordingly to computer data, including traffic data stored through computer systems held or under control of other persons. (8) Before completion of the criminal investigation, the prosecutor is under an obligation to inform in writing the persons against whom the criminal investigation is conducted and whose data 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.	*See the answer for article 16.* **Criminal Procedure Code** **Preservation of computer data (Art. 154)** (5) If data referring to information traffic is held by several providers of public electronic communication networks or providers of electronic communication services intended for the public, a provider holding or controlling the computer data is under an obligation to provide the criminal investigation bodies forthwith with the information necessary for the identification of other providers, in order to enable them to learn of all elements of the used communication chain.

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.	**Criminal Code** **SECTION 5** **Criminal investigation bodies and their competence of jurisdiction** ART. 55 - Criminal investigation bodies (1) Criminal investigation bodies are: a) prosecutors; b) criminal investigation bodies of the judicial police; c) special criminal investigation bodies. (2) Prosecutors are organized in prosecutors' offices that operate attached to courts of law and exercise their responsibilities within the Public Ministry. (3) In criminal proceedings, a prosecutor has the following responsibilities: a) to supervise or conduct the criminal investigation; b) to notify the Judge for Rights and Liberties and the court; c) to initiate and use criminal action; d) to initiate and use civil action, in situations established by law: e) to enter plea bargaining agreements, under the law; f) to file and use challenges and avenues of appeal set by the law against court decisions; g) to fulfil any other responsibilities set by law. […] (6) Criminal investigation bodies of the judicial police and special criminal investigation bodies perform their criminal investigation activities under the coordination and supervision of prosecutors. **Art.56 - Jurisdiction of prosecutors** (1) A prosecutor coordinates and controls directly criminal investigation activities performed by the judicial police and by special criminal investigation bodies set by law. Also, a prosecutor makes sure that criminal investigation acts are performed in compliance with the legal stipulations. (2) A prosecutor may perform any criminal investigation act in the cases they coordinate and supervise. […] **Art.152 - Obtaining data generated or processed by providers of public electronic communications networks or providers of electronic communication services intended for the public** (1) Criminal investigation bodies, subject to a prior authorization from the Judge for Rights and Liberties, may request a provider of public electronic

	communication networks or a provider of electronic communication services intended for the public to transmit the traffic or location data if the following cumulative conditions are fulfilled as such: (a) there is a reasonable suspicion in relation to the commission of an offense provided by Article 139 para. (2) or of an offense of disloyal competition, escape, counterfeiting documents, non-compliance with the rules governing weapons, ammunition, nuclear material and explosives, non-compliance with the rules governing introducing in the country waste and residues, an offence regarding organising and exploiting gambling or an offence related to drug precursors and offences related to operations with products with psychoactive effects similar to narcotic and psychotropic substances. b) there are grounds to believe that the requested data represent evidence. (c) evidence could not be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat for the safety of persons or of valuable goods. (d) the measure is proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offense; (2) The Judge for Rights and Liberties shall rule within 48 hours on requests transmitted by criminal investigation bodies regarding the transmission of data, through a reasoned court resolution, in chambers. (3) Providers of public electronic communication networks and providers of electronic communication services intended for the public that cooperate with criminal investigation bodies are under an obligation to keep secrecy of the conducted operations. **ART. 170 - Surrender of objects, documents or computer data** (1) In the event that there is a reasonable suspicion in relation to the preparation or commission of an offense and there are reasons to believe that an object or document can serve as evidence in a case, the criminal investigation bodies or the court may order the natural person or legal entity holding them to provide and surrender them, subject to receiving proof of surrender. (2) Also, under the terms of par. (1), criminal investigation bodies or the court may order: a) any natural person or legal entity on the territory of Romania to communicate specific computer data in their possession or under their control that is stored in a computer system or on a computer data storage medium; b) any provider of public electronic communication networks or provider of

	electronic communication services intended for the public to communicate specific data referring to subscribers, users and to the provided services that is in its possession or under its control, other than the content of communications and then those specified by Art. 138 par. (1) item j). (2^1) Natural persons or legal entities, including providers of public electronic communication networks or providers of electronic communication services intended for the public, can ensure the signing of the data requested under par. (2), by using an extended electronic signature based on a qualified certificate issued by an accredited certification service provider. (2^2) Any authorized person transmitting data requested under par. (2) can sign the transmitted data by using an extended electronic signature based on a qualified certificate issued by an accredited certification service provider, and which allows for an unambiguous identification of the authorized person, thus taking responsibility for the integrity of the transmitted data. (2^3) Any authorized person receiving data requested under par. (2) can check the integrity of the received data and certify such integrity by signing them, by means of an extended electronic signature based on a qualified certificate issued by an accredited certification service provider, and which allows for an unambiguous identification of the authorized person. (2^4) Each person certifying data based on an electronic signature shall be liable for the integrity and security of such data under the law. (2^5) The stipulations of par. (2^1) - (2^4) shall be applied by following the procedures set by the implementation regulations for the applicability of this 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	**Art. 168 – Computer search** (1) A computer system search or a computer data storage medium search designates the procedure for the investigation, discovery, identification and collection of evidence stored in a computer system or in a computer data storage medium, performed by means of adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these. (2) During a the criminal investigation, the Judge for Rights and Liberties of the court that would have the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office with which the prosecutor conducting or supervising the criminal investigation is working are located may order the conducting of a computer search, upon request by the prosecutor, when the investigation of a computer system or of a computer data storage medium is

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.	necessary for the discovery and collection of evidence. (3) The prosecutor shall submit an application requesting the approval of a computer search together with the case file to the Judge for Rights and Liberties. (4) Such application is ruled on in chambers, without summoning the parties. The prosecutor's attendance is mandatory. (5) The judge orders, through a court resolution, to sustain the application, when this is well-grounded, to approve the computer search, and issues a search warrant forthwith. (6) Such court resolution has to contain: a) name of the court; b) date, time and place of issuance; c) surname, first name and capacity of the person who issued the warrant; d) the time frame for which the warrant was issued and within which the ordered activity has to be performed; e) purpose for which it was issued; f) the computer system or computer data storage medium that is to be subject to search, as well as the name of the suspect or defendant, if known; g) signature of the judge and stamp of the court. (7) A court resolution through which the Judge for Rights and Liberties decides upon an application for the approval of a computer search is not subject to avenues of appeal. (8) In the event that, on the occasion of a search of a computer system or of a computer data storage medium, it is found that the sought computer data is stored in a different computer system or a computer data storage medium, and is accessible from the initial system or medium, the prosecutor shall immediately order the preservation and copying of the identified computer data and shall request the issuance of a warrant on an emergency basis. The stipulations of par. (1) - (7) shall apply accordingly. (9) In conducting the ordered search, in order to ensure integrity of the computer data stored on the seized objects, the prosecutor shall order the making of copies of them. (10) If the seizure of objects containing computer data set under par. (1) seriously hinders the performance of activities by the persons holding such objects, the prosecutor may order the making of copies of them, which would serve as methods of proof. Copies are made with adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these.

	(11) A computer system or computer data storage medium search is conducted in the presence of a suspect or a defendant, and the provisions of Art. 159 par. (10) and (11) shall apply accordingly. (12) A computer system or computer data storage medium search is conducted by a specialist working with the judicial bodies or an external one, in the presence of the prosecutor or of the criminal investigation bodies. (13) A computer search report has to contain: a) name of the person from whom a computer system or computer data storage media is seized or name of the person whose computer system is subject to search; b) name of the person having conducted the search; c) names of the persons present during the search conducting; d) a description and list of the computer systems or computer data storage media against which search was ordered; e) a description and list of the performed activities; f) a description and list of the computer data discovered on the occasion of the search; g) signature or stamp of the person having conducted the search; h) signature of the persons present during the search conducting. (14) Criminal investigation bodies have to take steps in order to make sure that the search is conducted without making facts and circumstances of the private life of the person subject to search public in an unjustified manner. (15) Computer data of a secret nature identified during such search is kept under the law. (16) During the trial, computer search is ordered by the court, ex officio or upon request by the prosecutor, by the parties or the victim, in the situations set by par. (2). A warrant for a computer search ordered by the court shall be communicated to the prosecutor, who shall act as per par. (8) - (15). **Art. 168^1 - Computer search by police officers** Computer search provided by art. 168 paragraph (12) can be performed also by specialised police officers specialised carried in the presence of the prosecutor or of the criminal investigation bodies.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be	See the answer for article 21

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	**CHAPTER IV** **Surveillance or investigation special methods** **ART. 138 - General provisions (see above)** **ART. 139 - Electronic surveillance** (1) Electronic surveillance is ordered by the Judge for Rights and Liberties when the following requirements are cumulatively met: a) there is a reasonable suspicion in relation to the preparation or commission of one of the offenses listed under par. (2); b) such measure is proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offense; c) evidence could not be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat for the safety of

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.	persons or of valuable goods. (2) Electronic surveillance may be ordered in case of offenses against national security stipulated by the Criminal Code and by special laws, as well as in case of drug trafficking, illegal operations with precursors or other products with psychoactive effects, non-compliance with the rules governing weapons, ammunition, nuclear material and explosives , trafficking and exploitation of vulnerable persons, acts of terrorism, money laundering, counterfeiting of currency, stamps or other values, counterfeiting electronic payment instruments in case of the offences committed through the computer systems or means of electronic communication, offenses against property, blackmail, rape, deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, offenses committed by means of computer systems or electronic communication devices, or in case of other offenses in respect of which the law sets forth a penalty of no less than 5 years of imprisonment. (3) The recordings set forth by this chapter, done by the parties or by other persons, represent evidence when they concern their own conversations or communications with third parties. Any other recordings may constitute evidence unless prohibited by law. (4) The relationship between a counsel and a person assisted or represented by them cannot be subject to electronic surveillance unless there is information that the counsel perpetrates or prepares the commission of any of the offenses listed under paragraph (2). If during or after the performance of such measure it results that the activities of electronic surveillance also targeted the relations between the counsel and the suspect or defendant defended by the former, the evidence obtained this way may not be used in a criminal proceeding, and shall be destroyed forthwith by the prosecutor. The judge having ordered such measure shall be informed forthwith by the prosecutor. When deemed necessary, the judge may order the information of the counsel. **ART. 140 - Procedure for the issuance of an electronic surveillance warrant** (1) Electronic surveillance may be ordered during the criminal investigation, for a term of maximum 30 days, upon request by the prosecutor, the Judge for Rights and Liberties of the court having the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office to which the prosecutor who filed the application belongs are located.

	(2) Such application filed by the prosecutor has to contain: the electronic surveillance measures that are requested for authorization, the name or the identification data of the person against whom such measure is to be ordered, if known, the evidence or data giving rise to a reasonable suspicion related to the commission of an offense in respect of which such measure may be ordered, the facts and the charges, and, in case of a video, audio or photo surveillance measure, whether an approval for criminal investigation bodies to enter private spaces indicated for activating and deactivating the technical devices to be used for the enforcement of the electronic surveillance measure is also requested, and a justification of the proportional and subsidiary nature of the measure. The prosecutor has to submit the case file to the Judge for Rights and Liberties. (3) An application requesting approval of electronic surveillance shall be ruled on in chambers, on the same day, without summoning the parties. The prosecutor's attendance is mandatory. (4) If they decide that the application is justified, the Judge for Rights and Liberties shall order admission of the prosecutor's application, through a court resolution, and shall issue forthwith a electronic surveillance warrant. Writing of a report is mandatory. (5) The court resolution of the Judge for Rights and Liberties and the warrant have to contain: a) name of the court; b) warrant issuance date, time and venue; c) surname, first name and capacity of the person returning the court resolution and issuing the warrant; d) description of the concrete approved measure; e) time period and purpose for which the measure was authorized; f) name of the person subject to a electronic surveillance measure or their identification data, if known; g) indication, if necessary given the nature of the approved measure, of the identification elements of each phone device, of the access point to a computer system, and of any known data for the identification of a communication channel or of an account number; h) in case of a measure of video, audio or photo surveillance in private spaces, mention of approving permission to criminal investigation bodies to enter private spaces in order to activate and deactivate the technical devices to be used for the enforcement of the electronic surveillance measure; i) signature of the judge and stamp of the court.

	(6) In the event that the Judge for Rights and Liberties decides that the requirements set by Art. 139 and The stipulations of par. (1) of this Article are not met, they shall deny the application for approving a electronic surveillance measure, through a court resolution. (7) A court resolution under which the Judge for Rights and Liberties rules on electronic surveillance measures is not subject to avenues of appeal. (8) A new application for the approval of the same measure may be filed only if new facts or circumstances, which were not known at the moment when the Judge for Rights and Liberties ruled on the previous application, occurred or were discovered. (9) Upon justified request by an victim, the prosecutor may request the judge to authorize the wiretapping or recording of communications, as well as of any types of communications performed by them through any communication device, irrespective of the nature of the offense subject to investigation. The stipulations of par. (1) - (8) shall apply accordingly. **ART. 141 - Authorization of electronic surveillance measures by the prosecutor** (1) The prosecutor may authorize, for a time period of maximum 48 hours, electronic surveillance measures when: a) there is an emergency situation, and the obtaining of a electronic surveillance warrant under the terms of Art. 140 would lead to a substantial delay of investigations, to the loss, alteration or destruction of evidence, or would jeopardize the safety of the victim, of witnesses or of their family members; and b) the requirements set by Art. 139 par. (1) and (2) are met. (2) A prosecutorial order authorizing electronic surveillance measures has to contain the mentions specified by Art. 140 par. (5). (3) Within a maximum of 24 hours following expiry of a measure, the prosecutor is under an obligation to notify the Judge for Rights and Liberties of the court having the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office to which the prosecutor who issued the order belongs are located, in order for them to confirm the measure and, at the same time, shall forward a report presenting a summary of the electronic surveillance activities performed and the case file. (4) If the Judge for Rights and Liberties decides that the requirements set by par. (1) were met, they shall confirm the measure ordered by the prosecutor within 24

	hours, through a court resolution, returned in chambers, without summoning the parties. (5) In respect of computer data identified through accessing a computer system, the prosecutor may order, through a prosecutorial order: a) making and preservation of a copy of such computer data; b) prohibition of access to or removal of such computer data from the computer system. Copies shall be made by means of appropriate technical devices and procedures, of nature to ensure the integrity of information contained by these. (6) If the Judge for Rights and Liberties decides that the requirements set by par. (1) were not met, they shall nullify the measure taken by the prosecutor and shall order destruction of the evidence thus obtained. The prosecutor shall destroy the evidence obtained this way and shall prepare a report in this sense. (7) Together with the application for a confirmation of their measure, or separately, the prosecutor may request the Judge for Rights and Liberties to warrant electronic surveillance measures under the terms of Art. 140. (8) A court resolution through which the Judge for Rights and Liberties rules on the measures ordered by the prosecutor is not subject to avenues of appeal. **ART. 142 - Enforcement of electronic surveillance warrants** (1) The prosecutor shall enforce an electronic surveillance measure or may order that this be enforced by criminal investigation bodies or by specialized employees of the law enforcement bodies or of other specialist bodies of the state. (2) Providers of public electronic communication networks or providers of electronic communication services intended for the public or of communication or financial services are under an obligation to cooperate with the criminal investigation bodies, the authorities listed under par. (1), within the limits of their authority, for the enforcement of electronic surveillance warrants. (3) Persons who are called to provide technical support for the enforcement of surveillance measures are under an obligation to keep secrecy in respect of the performed operation, under penalties set by the criminal law. (4) The prosecutor is under an obligation to cease electronic surveillance forthwith before expiry of the warrant term if the reasons justifying such measure no longer exist, by immediately informing the judge having issued the warrant. (5) Data resulted from electronic surveillance measures may be used also in other criminal case if they contain eloquent and useful data or information regarding the preparation or commission of another crime of those set forth by Art. 139 par.

	(2). (6) Data resulted from surveillance measures that do not concern the act subject to investigation or that do not contribute to the identification or locating of persons, if such are not used in other criminal cases as per par. (5), shall be archived at the premises of the prosecutors' office, in special places, by ensuring their confidentiality. Ex officio or upon request by the parties, the vested judge or judicial panel may request the sealed data if there is new evidence from which it results that part of these concern an act subject to investigation. One year after the final settlement of a case, these are destroyed by the prosecutor, who shall prepare a report in this sense. ART. 142^1 (1) Any authorized person conducting electronic surveillance activities, under this law, has the possibility to ensure the electronic signing of data resulting from electronic surveillance activities, by using an extended electronic signature based on a qualified certificate issued by an accredited certification services provider. (2) Any authorized person who transmits data resulting from electronic surveillance activities under this law, has the possibility to sign the transmitted data by using an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which allows for the unambiguous identification of the authorized person, the latter taking this way responsibility for the integrity of the transmitted data. (3) Any authorized person who receives data resulting from electronic surveillance activities under this law, has the possibility to check the integrity of the received data and to certify such integrity by signing them by means of an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which allows for the unambiguous identification of the authorized person. (4) Each person certifying data under electronic signature is liable for the security and integrity of such data under the law. **ART. 143 - Recording of electronic surveillance activities** (1) Prosecutors or criminal investigation bodies shall prepare a report for each electronic surveillance activity, in which they shall record the results of activities conducted in respect of an act subject to investigation or that contribute to the identification or localization of persons, the identification data of the medium containing the results of electronic surveillance activities, the names of persons to whom these refer, if known, or other identification data, as well as, as applicable,

	the date and time when such electronic surveillance activity started and the date and time when it ended. (2) A copy of the medium containing the results of electronic surveillance activities shall be attached to the reports, in a sealed envelope. Such medium or a certified copy of it shall be kept at the premises of the prosecutors' office, in special places, in a sealed envelope, and shall be made available to the court upon request. Following seizure of the court, a copy of the medium containing electronic surveillance activities and copies of the reports shall be kept at the court's registry office, in special places, in a sealed envelope, at the exclusive disposal of the judge or judicial panel vested with the case disposition. (2^1) Any authorized person making copies of a computer data storage medium containing results of electronic surveillance activities has the possibility to check the integrity of the data included in the original medium and, after making a copy, to sign the data included in it, by means of an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which allows for the unequivocal identification of the authorized person, the latter taking this way responsibility for the integrity of data. (3) Phone conversations, communications or discussions in a language other than Romanian shall be transcribed in Romanian, by means of an interpreter, who is under an obligation to keep their confidentiality. (4) Wiretapped and recorded phone conversations, communications or discussions concerning an act subject to investigation or which contribute to the identification or localization of persons, shall be transcribed by the prosecutor or the criminal investigation bodies in a report that shall mention the warrant issued for their conducting, the phone numbers, the identification data of computer systems or of access points, names of the persons who made such communications, if known, and the date and time of each conversation or communication. Such report shall be certified by the prosecutor for authenticity purposes. (5) After termination of a surveillance measure, the prosecutor shall inform the Judge for Rights and Liberties on the performed activities. **ART. 144 - Extension of an electronic surveillance warrant** (1) An electronic surveillance warrant may be extended, for well-grounded reasons, by the Judge for Rights and Liberties of the court of competent jurisdiction, upon reasoned request by the prosecutor, in situations where the requirements set by Art. 139 are met; however, each such extension may not

	exceed 30 days. (2) The Judge for Rights and Liberties shall rule in chambers, without summoning the parties, through a court resolution that is not subject to avenues of appeal. Preparation of a session minutes shall be mandatory. (3) The total duration of an electronic surveillance measure, related to the same person and the same act, may not exceed, in the same case, 6 months, except for the measure of video, audio or photo surveillance in private spaces, which may not exceed 120 days. **ART. 145 - Information of persons subject to surveillance** (1) Following termination of an electronic surveillance measure, the prosecutor shall inform each subject of the warrant for electronic surveillance enforced against them, in writing, within maximum 10 days. (2) Following such information, a person subject to surveillance has the right to learn, upon request, of the content of the minutes recording the electronic surveillance activities performed. Also, the prosecutor has to ensure, upon request, the listening to discussions, communications or conversations, or the watching of images resulted from each electronic surveillance activity. (3) The term for filing a request in this sense is of 20 days as of the date of communication of the written information set under par. (1). (4) The prosecutor may postpone such information or the presentation of media on which electronic surveillance activities are stored or the minutes transcribing them, in a justified way, if this could result in: a) disruption or jeopardizing of the proper conducting of the criminal investigation in the case; b) jeopardizing of the safety of the victim, witnesses or members of their families; c) difficulties in the electronic surveillance of other persons involved in the case. (5) The postponement set under par. (4) may be ordered until completion of the criminal investigation or until the case closure, at the latest. **ART. 146 - Preservation of materials resulted from electronic surveillance** (1) If a decision to close a case was returned in a case, against which a complaint was not filed within the legal term set by Art. 340 or such complaint was denied, the prosecutor shall inform the Judge for Rights and Liberties of this forthwith. (2) The Judge for Rights and Liberties shall order preservation of the material medium or of the certified copy of it, by archiving it at the premises of the court, in special places, in a sealed envelope, in order to ensure confidentiality. (3) If in a case the court returned a conviction sentence, a waiver of penalty or penalty reprieve, an acquittal or a termination of criminal proceedings, which

	remained final, the material medium or its copy shall be preserved by being archived together with the case file at the premises of the court, in special places, by ensuring confidentiality.
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. 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.	**Criminal Code** **SECTION 2** **Applicability of criminal law in space** **Art. 8 - Territoriality of criminal law** (1) Romanian criminal law applies to offenses committed on the territory of Romania. (2) The territory of Romania is defined as the expanse of land, the territorial sea waters and inland waters, complete with the soil, sub-soil and airspace located inside the national borders. (3) An offense committed on the territory of Romania is defined as any offense committed on the territory defined at par. (2) or on a ship sailing under Romanian pavilion or on an aircraft registered in Romania. (4) The offense is also considered as having been committed on the territory of Romania when on that territory or on a ship sailing under Romanian pavilion or on an aircraft registered in Romania an action was committed with a view to perform, instigate or aid in the offense, or the results of the offense have been manifest, even if only in part. **Art. 9 - Legal standing under criminal law** (1) Romanian criminal law applies to offenses committed outside Romanian territory by a Romanian citizen or a Romanian legal entity if the sentencing stipulated by Romanian law is life imprisonment or a term of imprisonment longer than 10 years. (2) In the other cases Romanian criminal law applies to offenses committed outside Romanian territory by a Romanian citizen or a Romanian legal entity if the act is also criminalized by the criminal law of the country where it was committed or if it was committed in a location that is not subject to any State's jurisdiction. (3) A criminal investigation can start on receiving authorization from the Chief Prosecutor of the Prosecutor's Office attached to the Court of Appeals in whose jurisdiction the first Prosecutor's Office is located that received information about the violation, or, as the case may be, from the Prosecutor General of the Prosecutor's Office attached to the High Court of Review and Justice. A prosecutor

	is entitled to issue such authorization within 30 days of receiving the application for authorization; such deadline can be extended, under the law, but for no more than a total of 180 days. **Art. 10 - Reality of criminal law** (1) Romanian criminal law applies to offenses committed outside Romanian territory by a foreign citizen or a stateless person against the Romanian State, against a Romanian citizen or against a Romanian legal entity. (2) A criminal investigation can start on receiving authorization from the Prosecutor General of the Prosecutor's Office attached to the High Court of Review and Justice, and only if the violation is not the object of judicial procedures that are already ongoing in the State on whose territory it was committed. **Art. 11*) - Universality of criminal law** (1) Romanian criminal law also applies to other violations than those stipulated at Art. 10, committed outside Romanian territory by a foreign citizen or a stateless person who is located voluntarily on Romanian territory, in the following cases: a) an offense was committed that the Romanian State has undertaken to repress on the basis of an international treaty, irrespective of whether it is stipulated by the criminal law of the State on whose territory it was committed; b) extradition or surrender of the offender has been requested and denied. (2) The stipulations of par. (1) lett. b) do not apply when, under the law of the state on whose territory the violation was committed, there is a cause to prevent the start of criminal action or the continuing of the criminal trial or the serving of the sentence or when the sentence has been served or when the sentence is considered as having been served. (3) When the sentence has not been served or has only been served in part, the applicable procedure is that of the law on the recognition of foreign judgments. *) Under Art. 237 in Law #187/2012 (#M3), in applying the stipulations of Art. 11 in the Criminal Code the condition of voluntary presence on Romanian territory shall be interpreted in the sense of the person being on said territory voluntarily at the date when the judicial bodies rule to deprive that person of their freedom or restrict that person's freedom in view of the offense that entails applicability of the principle of universality. **Art. 12 - Criminal law and the international treaties** The stipulations of Art. 8 – 11 shall apply unless otherwise required under an international treaty Romania is a party to.
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 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.	**Art. 96 of Law no. 302/2004 on the international cooperation in criminal matters** provides a list of 32 offences for which the double criminality check is lifted. Cybercrime, sexual exploitation of children and forgery of means of payment are on the list. Most of the offences comply with the 3 years threshold. Moreover, often there are several cybercrime offences committed or several material acts or the offence is committed together with participation into an organized criminal group. Therefore the 3 years threshold is most likely always met. Law no. 302/2004 establishes in Art. 26 that the seriousness of the offence is the criteria to be taken into account in order to establish whether an offence is extraditable. So in this case, Romania is not operating with a list of offences anymore. There are two thresholds established - one of at least one year-if the extradition is sought in order to criminal prosecute or trial a person and one of 4 months-if the extradition is requested in order to execute a punishment. The **surrender procedure** under the Framework Decision on the European Arrest Warrant and surrender procedure between the Member-States establishes the direct contact between Issuing and Executing judicial authorities. This principle has been taken over by the Romanian legislation. The Ministry of Justice as central authority rarely intervenes in the process, playing a mere administrative role (facilitating contact when needed or providing consultancy at the request of both Romanian judicial authorities and the foreign authority). The authorities competent to receive EAWs are the Prosecutor's Offices attached by the Courts of Appeal, while the authorities competent to execute the EAWs are the Romanian courts of appeal. Regarding the issuing of an EAW, depending on the type of offence, all Romanian courts could become involved (based on the material competence established by the Romanian Criminal Procedural Code). For the statements made by Romania and the list of competent authorities please find relevant data under: http://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=331 The authority responsible for sending and receiving extradition requests is the Ministry of Justice, which is performing regularity check for issuing and executing authorities.

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	Extradition requests and/or EAW are treated as a matter of urgency, the Romanian law establishing strict deadlines in this respect, whether the request is active or passive (corroborated with other legal instruments applicable). For example, in respect of the execution of the EAW the Romanian law establishes a maximum period of 90 days. If the person consents the surrender decision is pronounced within 10 days.
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	MLA requests for cybercrime cases are executed based on the law on international judicial cooperation in criminal matters (Law no. 302/2004) and the provisions of the Law no. 161/2003 (Chapter 5). In addition, bearing in mind the constitutional provisions that state that treaties once ratified become part of the domestic law, various regional and international treaties can be used as legal basis for cooperation with EU or third countries. **Law 161/2003** **Chapter V - International Cooperation** Art.60 – (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. Art.61 – (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 in paragraph (1) are carried out on the basis of bilateral or multilateral agreements concluded with the competent authorities.

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.	(3) The representatives of the Romanian competent authorities can participate in common investigations performed on the territory of other states by observing their legislation. **Law No. 302/2004 on international judicial cooperation in criminal matters** provides in art. 4 the pre-eminence of international law, stipulating that Law No. 302/2004 is applied on the basis and for the execution of norms related to international judicial cooperation in criminal matters included in international legal instruments to which Romania is a party to. Therefore, the domestic law applies only to establish norms where such norms have not been already been regulated by the international treaty or to complete them as the case may be. Law No. 302/2004 on international judicial cooperation in criminal matters represents the general framework in relation to international judicial cooperation in criminal matters. Law No. 161/2003 (Title III-Prevention and combatting cybercrime-Chapter 5), which implements the Convention on cybercrime, provides specific provisions related to cybercrime requests. In case of third countries, usually based on the legal treaty applicable, two situations can be encountered in relation to central authorities competent to send/received the MLA request: - two central authorities: the Public Ministry for MLA requests issued during investigation and criminal prosecution stage and the Ministry of Justice for requests issued during trial and execution stage or - one central authority: the Ministry of Justice if the request has been issued in the absence of a treaty and based on reciprocity or if the treaty applicable designates the Ministry of Justice as the single central authority. In addition, for requests related to criminal records, which are registered differently than MLA, the central authority is the Ministry of Internal Affairs. The competences of each central authority are established in the domestic law by Art. 10 of Law no. 302/2004. Regarding the decisions on such requests, the execution of the requests the judiciary is competent depending on the type of request and the stage of the trial (investigation and prosecution, or trial/execution stage). With reference to the channels of communication, usually, at EU level there is a

	direct channel used between the issuing and executing judicial authorities. In the process of international judicial cooperation at multilateral level, Romania is using the European Union Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union in conjunction MLA Conventions of the Council of Europe, Convention on Cybercrime or the United Nations Convention against Transnational Organized Crime, as the case may be.
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.	**Law 161/2003** **Art. 66** – 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. **Law no. 302/2004 on the international judicial cooperation in criminal matters** **ART. 179 - Spontaneous transmission of information** (1) The Romanian judicial authorities may, without prior request, forward to the competent authorities of a foreign State the information obtained within an inquiry, when they consider that the disclosure of such information might assist the receiving State in initiating a criminal procedure, or when the information might lead to the filing of a request for judicial assistance. (2) The Romanian State may impose certain conditions on the manner of use of the information transmitted, according to paragraph (1). The receiving State shall be bound by the conditions imposed.
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	*See the answer for Article 25*

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	Law no. 302/2004 on the international judicial cooperation in criminal matters

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.	
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:	*See also the relevant domestic provisions* **Law 161/2003** Art. 63 - (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; 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; Law no. 302/2004 on the international judicial cooperation in criminal matters

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 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.	*See also the relevant domestic provisions* **Law 161/2003** Art.64 - 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. **Law no. 302/2004 on the international judicial cooperation in criminal matters**
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	*See also the relevant domestic provisions* **Law 161/2003** **Chapter V - International Cooperation** Art.60 – (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the

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.	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. **Law no. 302/2004 on the international judicial cooperation in criminal matters**
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.	**Law 161/2003** Art.65 - (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 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.	*See also the relevant domestic provisions* Art. 60 Law no 161/2003 Law no. 302/2004 on the international judicial cooperation in criminal matters
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.	*See also the relevant domestic provisions* **Art. 60 Law no 161/2003** **Law no. 302/2004 on the international judicial cooperation in criminal matters** **ART. 184 - Interception and recording of conversations and**

	communications (1) In view of solving a criminal case, the judicial authorities of the requesting State or the competent authorities thus designated by the requesting State can address to the Romanian authorities a request for judicial assistance having as object the interception of telecommunications and their immediate transmission to the requesting State or the interception of the recording and of the subsequent transmission of the recording of telecommunications to the requesting State, in case the prosecuted person: a) is on the territory of the requesting State and the latter needs technical assistance to intercept communications from the target; b) is on the territory of territory of Romania, in the event that the communications from the target can be intercepted in the Romanian State; c) is on the territory of a third country which has been informed also whether the requesting State needs technical assistance for intercepting communications from the target. (2) The requests submitted for the application of this Article must meet the following conditions: a) specify and confirm the issuing of an order or a warrant for interception and recording, within a criminal trial; b) contain information that would allow identification of the target of the interception; c) indicate the criminal acts that are the object of the criminal investigation; d) mention the duration of interception; e) if possible, contain sufficient technical data, in particular the number for connecting to the network, in order to allow the processing of the request. (3) Where the request is formulated in compliance with the provisions of paragraph (1) b), it must contain also a description of the facts. The Romanian judicial authorities may request any other additional information needed to allow them to establish whether the requested measure would also have been taken in a similar national case.
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	To ensure the immediate and permanent international cooperation in combating cybercrime, Art. 62 of Law No. 161/2003 established a permanently available point of contact within the Service for Combating Cybercrime, Department for Combating Organised Crime and Drug Trafficking from the Prosecutor`s Office of the Supreme Court of Justice. Later on by Law No. 504 /2008 a 24/7 contact point was incorporated within the

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.	Service for Preventing and Combating Cybercrime of the Directorate for Investigating Organized Crime and Terrorism Offences, which is a specialised structure of the Prosecutor's Office attached to the High Court of Cassation and Justice. The Service for Preventing and Combating Cybercrime has the following responsibilities: a. grants specialised assistance and provides data about the Romanian legislation on similar contact points in other states; b. orders the immediate preservation of data, and the lifting of objects containing computer data or information related to traffic data requested by a competent foreign authority; c. carries out or facilitates the application, according to the law, of letters rogatory required in cases of combating cybercrime, by cooperating with all the relevant Romanian authorities. Within the Police, there is a secondary 24/7 point of contact to assist the existing one from the Prosecutor's Office. This point of contact is the Service for combating Cybercrime, where designated personnel take incoming requests and process them. The two points of contact from the Police and the Prosecutor`s Office keep in touch and coordinate their activities on urgent requests. The point of contacts has e-mail address, a cell phone and a fixed phone, as well as a fax line in order to ensure taking requests.
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.	*No reservations*