



Cybercrime legislation – country profile

REPUBLIC OF SERBIA

This profile has been prepared within the framework of the EU/COE Joint Project on Regional Cooperation against Cybercrime in South-eastern Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the 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:

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

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

Country:	Republic of Serbia
Signature of Convention:	07/04/2005
Ratification/accession:	14/04/2009
Provisions of the Convention	Corresponding provisions/solutions in national legislation <i>(pls quote or summarise briefly; pls attach relevant extracts as an appendix)</i>
Chapter I – Use of terms	
Article 1 – “Computer system”, “computer data”, “service provider”,	In Chapter 12, article 112 of Criminal Code of Republic of Serbia (CCRS), in

<p>“traffic data”: For the purposes of this Convention:</p> <p>a “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;</p> <p>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;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>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</p>	<p>paragraph 17, 18, 19 and 20, terms: computer data, Computer program, computer virus and computer network are explained. The terms: “computer system, “Service provider” and “traffic data” are not provided.</p> <p>Article 112 - Meaning of Terms for the Purpose of this Code</p> <p>(17) Computer data is presented information, knowledge, fact, concept or order that is entered, processed or memorised or has been entered, processed or memorised in a computer or computer network.</p> <p>(18) A computer network is an assembly of mutually interconnected computers that communicate with each other by exchanging data.</p> <p>(19) A computer program is a regulated assembly of orders serving to control computer operation, as well as to solve a specific task by means of a computer.</p> <p>(20) A computer virus is a computer program or some other group of orders entered into a computer or computer network designed to multiply itself and act on other programs or data in a computer or a computer network by adding that program or group of orders to one or more computer programs or data.</p> <p>amendment 11/9/2009 “Official gazette of Republic Serbia 72/2009”</p> <p>(17) Computer data is any representation of facts, information or concepts in form which is suitable for their processing in computer system including suitable program on base which computer system is managing its function.</p> <p>(18) A computer network is an assembly of mutually interconnected computers or computers systems that communicate with each other by exchanging data.</p> <p>(33) Computer is every electronic device which is, based on program, automatically processing and exchanging data.</p> <p>(34) Computer system is every device or group of interconnected or dependent units of which one or more, based on program, performs automatic data processing.</p>
<p>Chapter II – Measures to be taken at the national level Section 1 – Substantive criminal law</p>	
<p><i>Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems</i></p>	
<p>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</p>	<p>In Chapter 27 at article 302 of CCRS “Illegal access to protected computer, computer network and electronic processing of data” is provided as specific criminal offence.</p>

<p>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.</p>	<p>Article 302 - Unauthorised Access to Computer, Computer Network or Electronic Data Processing</p> <p>(1) Whoever, by circumventing protection measures, accesses a computer or computer network without authorisation, or accesses electronic data processing without authorisation, shall be punished by fine or imprisonment up to six months.</p> <p>(2) Whoever uses data obtained in manner provided under paragraph 1 of this Article, shall be punished by fine or imprisonment up to two years.</p> <p>(3) If the offence specified in paragraph 1 of this Article results in hold-up or serious malfunction in electronic processing and transfer of data or of the network, or other grave consequences have resulted, the offender shall be punished by imprisonment up to three years.</p> <p>amendment 11/9/2009</p> <p>(2) Whoever records or uses data obtained in manner provided under paragraph 1 of this Article, shall be punished by fine or imprisonment up to two years.</p>
<p>Article 3 – Illegal interception</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p>In Chapter 27 at article 298 “Damaging of computer data and programs” illegal interception is covered in the first paragraph.</p> <p>not amendment</p>
<p>Article 4 – Data interference</p> <p>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.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p>In Chapter 27 at the article 300, paragraph 1 and 2 of CCRS, “Creating and inserting computer viruses” is provided as specific criminal offence.</p> <p>Article 298 - Damaging Computer Data and Programs</p> <p>(1) Whoever without authorisation deletes, alters, damages, conceals or otherwise makes unusable a computer datum or program, shall be punished by fine or imprisonment up to one year.</p> <p>(2) If the offence specified in paragraph 1 of this Article results in damages exceeding four hundred and fifty thousand dinars, the offender shall be punished</p>

	<p>by imprisonment of three months to three years. (3) If the offence specified in paragraph 1 of this Article results in damages exceeding one million five hundred thousand dinars, the offender shall be punished by imprisonment of three months to five years. (4) Equipment and devices used in perpetration of the offence specified in paragraphs 1 and 2 of this Article shall be seized.</p> <p>not amendment</p>
<p>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</p>	<p>This is provided in articles: 299 (“Computer sabotage”) and 300 (“Creating and inserting of computer viruses”).</p> <p>Article 299 - Computer Sabotage Whoever enters, destroys, deletes, alters, damages, conceals or otherwise makes unusable computer datum or program or damages or destroys a computer or other equipment for electronic processing and transfer of data, with intent to prevent or considerably disrupt the procedure of electronic processing and transfer of data that are of importance for government authorities, enterprises or other entities, shall be punished by imprisonment of six months to five years.</p> <p>not amendment</p>
<p>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</p>	<p>This is provided in article 300 paragraph 1, 2 and 3 and article 302 1 and 2 of CRRS (“Unauthorized access to protected computer, computer network and electronic data processing”).</p> <p>Article 300 - Creating and Introducing of Computer Viruses (1) Whoever makes a computer virus with intent to introduce it into another’s computer or computer network, shall be punished by fine or imprisonment up to six months. (2) Whoever introduces a computer virus into another’s computer or computer network thereby causing damage, shall be punished by fine or imprisonment up to two years. (3) Equipment and devices used for committing of the offence specified in paragraphs 1 and 2 of this Article shall be seized.</p>

<p>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.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p> <p>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.</p>	<p>not amendment</p> <p>Article 302 - Unauthorised Access to Computer, Computer Network or Electronic Data Processing</p> <p>(1) Whoever, by circumventing protection measures, accesses a computer or computer network without authorisation, or accesses electronic data processing without authorisation, shall be punished by fine or imprisonment up to six months.</p> <p>(2) Whoever uses data obtained in manner provided under paragraph 1 of this Article, shall be punished by fine or imprisonment up to two years.</p> <p>(3) If the offence specified in paragraph 1 of this Article results in hold-up or serious malfunction in electronic processing and transfer of data or of the network, or other grave consequences have resulted, the offender shall be punished by imprisonment up to three years.</p> <p>amendment like above</p>
<p><i>Title 2 – Computer-related offences</i></p>	
<p>Article 7 – Computer-related forgery</p> <p>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.</p>	<p>This is provided in article 301 of CCRS.</p> <p>Article 301 - Computer Fraud</p> <p>(1) Whoever enters incorrect data, fails to enter correct data or otherwise conceals or falsely represents data and thereby affects the results of electronic processing and transfer of data with intent to acquire for himself or another unlawful material gain and thus causes material damage to another person, shall be punished by fine or imprisonment up to three years.</p> <p>(2) If the offence specified in paragraph 1 of this Article results in acquiring material gain exceeding four hundred and fifty thousand dinars, the offender shall be punished by imprisonment of one to eight years.</p> <p>(3) If the offence specified in paragraph 1 of this Article results in acquiring material gain exceeding one million five hundred thousand dinars, the offender shall be punished by imprisonment of two to ten years.</p> <p>(4) Whoever commits the offence specified in paragraph 1 of this Article from malicious mischief, shall be punished by fine or imprisonment up to six months.</p> <p>not amendment</p>
<p>Article 8 – Computer-related fraud</p>	<p>Also, provided in article 301 of CCRS.</p>

<p>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:</p> <ul style="list-style-type: none"> a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p>Article 301 - Computer Fraud</p> <p>(1) Whoever enters incorrect data, fails to enter correct data or otherwise conceals or falsely represents data and thereby affects the results of electronic processing and transfer of data with intent to acquire for himself or another unlawful material gain and thus causes material damage to another person, shall be punished by fine or imprisonment up to three years.</p> <p>(2) If the offence specified in paragraph 1 of this Article results in acquiring material gain exceeding four hundred and fifty thousand dinars, the offender shall be punished by imprisonment of one to eight years.</p> <p>(3) If the offence specified in paragraph 1 of this Article results in acquiring material gain exceeding one million five hundred thousand dinars, the offender shall be punished by imprisonment of two to ten years.</p> <p>(4) Whoever commits the offence specified in paragraph 1 of this Article from malicious mischief, shall be punished by fine or imprisonment up to six months.</p> <p>not amendment</p>
<p><i>Title 3 – Content-related offences</i></p>	
<p>Article 9 – Offences related to child pornography</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:</p> <ul style="list-style-type: none"> a a minor engaged in sexually explicit conduct; 	<p>Partially article 185 Penal code, but possession of these material isn’t criminal offense and there is a problem in defining a category of minors (under 14 only)</p> <p>Article 185 - Showing Pornographic Material and Child Pornography</p> <p>(1) Whoever sells, shows or publicly displays or otherwise makes available texts, pictures, audio-visual or other items of pornographic content to a child or shows to a child a pornographic performance, shall be punished with a fine or imprisonment up to six months.</p> <p>(2) Whoever uses a child to produce photographs, audio-visual or other items of pornographic content or for a pornographic show, shall be punished with imprisonment from six months to five years.</p> <p>(3) Whoever sells, shows, publicly exhibits or electronically or otherwise makes available pictures, audio-visual or other items of pornographic content resulting from offences specified in paragraph 2 of this Article, shall be punished with imprisonment up to two years.</p> <p>(4) Items specified in paragraphs 1 through 3 of this Article shall be confiscated.</p> <p>amendment 11/9/2009</p>

<p>b a person appearing to be a minor engaged in sexually explicit conduct;</p> <p>c realistic images representing a minor engaged in sexually explicit conduct</p> <p>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.</p> <p>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.</p>	<p>(1) Whoever to juvenile sells, shows or publicly displays or otherwise makes available texts, pictures, audio-visual or other items of pornographic content to a child or shows to a child a pornographic performance, shall be punished with a fine or imprisonment up to six months.</p> <p>(2) Whoever uses a juvenile to produce photographs, audio-visual or other items of pornographic content or for a pornographic show, shall be punished with imprisonment from six months to five years.</p> <p>(3) If actions from paragraph 1. and 2. of this article are committed against child offender shall be punished for paragraph 1. with imprisonment from six months to three years, and for action from paragraph 2. with imprisonment from one to eight years.</p> <p>(4) Whoever obtains for himself or another, possess, sells, shows, publicly exhibits or electronically or otherwise makes available pictures, audio-visual or other items of pornographic content resulting from exploitation of minor shall be punished with imprisonment from three months to three years.</p> <p>(5) Items specified in paragraphs 1 through 4 of this Article shall be confiscated.</p> <p style="text-align: center;">Article 185 b Usage of computer network or communication with other technical resources for committing crimes against sexual freedom toward minor</p> <p>(1)Whoever in intent of committing crimes from Art.178. par.4, 179. par.3, 180. par. 1. and 2, 181. par. 2. and 3, 182. par. 1, 183. par.2, 184. par.3, 185. par.2. and 185a of this code using computer network or communication with other technical resources agreed to a minor meeting and show up at the agreed place because of a meeting shall be punished with imprisonment from six months to five years and fine.</p> <p>(2)Whoever action from par 1. commits toward a child shall be punished with imprisonment from one to eight years.</p>
<i>Title 4 – Offences related to infringements of copyright and related rights</i>	
<p>Article 10 – Offences related to infringements of copyright and related rights</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the</p>	<p>Those are offences provided in the Chapter 20, at the article 199 named as "Unauthorized exploitation of copyright or the subject of related right", paragraph 1 and 2 ; as well as, article 200, named as " Unauthorized removing and changing electronic information about copyright and related rights",</p>

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.

paragraph 1.

CHAPTER TWENTY CRIMINAL OFFENCES AGAINST INTELLECTUAL PROPERTY

Article 199 - Unauthorised Use of Copyrighted Work or other Work Protected by Similar Right

(1) Whoever without permission publishes, records, copies or otherwise presents in public, in part or entirety, a copyrighted work, performance, phonogram, videogram, show, computer programme or database, shall be punished with a fine or imprisonment up to three years.

(2) The punishment specified in paragraph 1 of this Article shall also be imposed on a person who puts into circulation or with intent to put into circulation keeps illegally multiplied or illegally put into circulation copies of copyrighted work, performance, phonogram, videogram, show, computer program or database.

(3) If the offence referred to in paragraphs 1 and 2 of this Article was committed with intent to acquire material gain for oneself or another, the offender shall be punished with imprisonment from three months to five years.

(4) Whoever produces, imports, puts into circulation, sells, rents, advertises for sale or renting, or keeps for commercial purposes, equipment and devices whose basic or prevailing purpose is to remove, bypass or forestall technological measures intended for prevention of violation of copyright and other similar rights, or who uses such equipment or devices with an aim to violate copyright or other similar right, shall be punished with a fine or imprisonment up to three years.

(5) The things referred to in paragraphs 1 through 4 shall be seized and destroyed.

amendment 11/9/2009

(2) The punishment specified in paragraph 1 of this Article shall also be imposed on a person who puts into circulation or with intent to put into circulation **keeps** illegally multiplied or illegally put into circulation copies of copyrighted work, performance, phonogram, videogram, show, computer program or database.

3) If the offence referred to in paragraphs 1 and 2 of this Article was committed with intent to acquire material gain for oneself or another, the offender shall be punished with imprisonment from **six** months to five years.

<i>Title 5 – Ancillary liability and sanctions</i>	
<p>Article 11 – Attempt and aiding or abetting</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>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.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	<p>Article 30 paragraph 1 and 2 of the CCRS is applied. It is only concerning the article 301, paragraph 2 and 3 (Computer forgery). Aiding and abetting are covered in article 34 and 35 of CCRS.</p> <p>Article 30 - Attempt</p> <p>(1) Whoever commences a criminal offence with premeditation, but does not complete it, shall be punished for the attempted criminal offence if such offence is punishable by law with a term of imprisonment of five years or more, and for the attempt of other criminal offence only when the law explicitly provides for the punishment of attempt.</p> <p>(2) A perpetrator shall be punished for an attempt with a punishment prescribed for the criminal offence or with a lighter punishment.</p> <p>not amendment</p> <p>Complicity in Criminal Offence</p> <p>Article 33 - Co-perpetration</p> <p>If several persons jointly take part in committing a criminal offence, or jointly commit an offence out of negligence, or by carrying out a jointly made decision, by other premeditated act significantly contribute to committing a criminal offence, each shall be punished as prescribed by law for such offence.</p> <p>not amendment</p> <p>Article 34 - Incitement</p> <p>(1) Whoever with intent incites another to commit a criminal offence shall be punished as prescribed by law for such offence.</p> <p>(2) Whoever with intent incites another to commit a criminal offence whose attempt is punishable by law, and such offence has not been attempted at all, shall be punished as for the attempted criminal offence.</p> <p>not amendment</p>

	<p>Article 35 - Aiding and Abetting</p> <p>(1) Anyone aiding another with intent in committing a criminal offence shall be punished as prescribed by law for such criminal offence, or by a mitigated penalty.</p> <p>(2) The following, in particular, shall be considered as aiding in the commission of a criminal offence: giving instructions or advice on how to commit a criminal offence; supply of means for committing a criminal offence; creating conditions or removal of obstacles for committing a criminal offence; prior promise to conceal the commission of the offence, offender, means used in committing a criminal offence, traces of criminal offence and items gained through the commission of criminal offence.</p> <p>not amendment</p>
<p>Article 12 – Corporate liability</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	<p>In CCRS the corporate liability is not yet established</p> <p><i>From 4/11/2008 Law on corporate liability has been entered into force.</i></p>
<p>Article 13 – Sanctions and measures</p> <p>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</p>	<p>Proportionate and dissuasive sanctions, which include, monetary sanctions and deprivation of liberty are included.</p>

dissuasive sanctions, which include deprivation of liberty.

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

Section 2 – Procedural law

Article 14 – Scope of procedural provisions

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

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

- a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
- b other criminal offences committed by means of a computer system; and
- c the collection of evidence in electronic form of a criminal offence.

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

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

- i is being operated for the benefit of a closed group of users, and
- ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such

Procedural provisions are covered in Criminal Procedural Code, and The Law on Organization and Jurisdiction of State Authorities for Combating High- Tech Criminality.

<p>communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21</p>	
<p>Article 15 – Conditions and safeguards</p> <p>1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.</p> <p>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.</p> <p>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.</p>	<p>The provisions of Criminal Procedural Law (CPC) which are generally being harmonized with international standards are applied.</p>
<p>Article 16 – Expedited preservation of stored computer data</p> <p>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.</p> <p>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</p>	<p>It is not directly prescribed, but general provisions of article 85 paragraph 1, 146 paragraph 1 and 7, article 155, and 255 paragraph 2, can be applied.</p> <p>ARTICLE 85</p> <p>(1) The investigating judge may order on his own initiative or upon the motion of the State Attorney that postal, telephone and other communication agencies retain and deliver to him, against a receipt, letters, telegrams and other shipments addressed to the defendant or sent by him if circumstances exist which indicate that it is likely that these shipments can be used as evidence in the proceedings.</p> <p>(2) The shipments shall be opened by the investigating judge in the presence of two witnesses. When opening, care shall be taken not to damage the seals, while the covers and addresses shall be preserved. A record shall be drawn up on the opening.</p>

disclosure. A Party may provide for such an order to be subsequently renewed.

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

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

(3) If the interests of the proceedings so allow, the defendant or the addressee may be fully or partially informed of the contents of the shipment, which may be delivered to him as well. If the defendant is absent, the shipment shall be returned to the sender unless this would prejudice the interests of the proceedings.

amendment 11/9/2009 "Official gazette of Republic Serbia 72/2009"
(4) Measures referred to par 1 of this article shall be reviewed every three months and can last up to nine months. Implementation of measures will be stopped as soon as the reasons for their application are ceased.

ARTICLE 146

(1) After the indictment has been submitted to the court and up to the closing of the trial, detention may be ordered or vacated only by the ruling rendered by the panel, provided that the opinion of the State Attorney is obtained if the proceedings are conducted upon his request.

(2) Even without motion submitted by parties, the panel is bound to review whether the grounds for detention still exist and to prolong or vacate it by a ruling every month from the moment the last ruling on detention becomes finale, and every two months from the moment the indictment becomes final.

(3) After the indictment is preferred detention may last two years at the longest. If within this period a judgment at first instance fails to be pronounced, detention shall be vacated and a detainee released.

(4) After the judgment at first instance is imposed, detention may last one year at the longest. If within this period a judgment at second instance, by which the judgment at first instance is revised or affirmed, is not rendered, detention shall be vacated and the accused released. If within a term of one year a court at second instance renders a judgment vacating the judgment at first instance, detention may last at the longest for one more year from the day the judgment at second instance is rendered.

(5) An appeal on the ruling referred to in paragraphs 1 and 2 of this Article does not stay the execution of the ruling.

(6) The ruling of the panel by which the motion to order or vacate detention is rejected is not appealable.

amendment

	<p><i>(1) After the indictment has been submitted to the court and up to the closing of the trial decision of the appointment, extension or termination of custody is brought under Art 142a of this code.</i></p> <p>ARTICLE 255</p> <p>(1) Before the conclusion of the investigation, the investigating judge shall obtain information on the defendant stated in Article 89 paragraph 1 of this Act if they are missing or require a review, as well as information on the defendant's previous convictions and, if he is still serving a sentence or another sanction which is connected to deprivation of liberty - information on his behavior while serving the sentence or other sanction. If necessary, the investigating judge shall obtain information on the defendant's previous life, on the circumstances under which he lives and on other circumstances concerning his personality. The investigating judge may order a medical or psychological examination of the defendant when it is necessary to supplement information on the defendant's personality.</p> <p>(2) If it is possible to impose an aggregate sentence comprising the sentence from previous judgments as well, the investigating judge shall require the files containing these judgments or certified copies of the final judgments.</p> <p><i>amendment and brought back to this solution</i></p>
<p>Article 17 – Expedited preservation and partial disclosure of traffic data</p> <p>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:</p> <p>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</p> <p>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.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>For these purposes article 84, and 85 paragraph 2,3 and 4, and 147 paragraph 2 of CPC can be applied.</p> <p>ARTICLE 84</p> <p>(1) When files of evidentiary value are temporarily seized, a list of them shall be made. If this is not possible, the files shall be put in a cover and sealed. The owner of the files may put his own seal on the cover.</p> <p>(2) The person from whom the files have been seized shall be summoned to attend the opening of the cover. If this person fails to appear or is absent the cover shall be opened, the files examined and a list of them made in his absence.</p> <p>(3) When examining files, unauthorized persons should not have access to their contents.</p> <p>not amendment</p>

	<p>ARTICLE 85</p> <p>(1) The investigating judge may order on his own initiative or upon the motion of the State Attorney that postal, telephone and other communication agencies retain and deliver to him, against a receipt, letters, telegrams and other shipments addressed to the defendant or sent by him if circumstances exist which indicate that it is likely that these shipments can be used as evidence in the proceedings.</p> <p>(2) The shipments shall be opened by the investigating judge in the presence of two witnesses. When opening, care shall be taken not to damage the seals, while the covers and addresses shall be preserved. A record shall be drawn up on the opening.</p> <p>(3) If the interests of the proceedings so allow, the defendant or the addressee may be fully or partially informed of the contents of the shipment, which may be delivered to him as well. If the defendant is absent, the shipment shall be returned to the sender unless this would prejudice the interests of the proceedings.</p> <p><i>amendment like above</i></p> <p>ARTICLE 147</p> <p>(1) The police authority or the court is bound immediately after a person has been deprived of liberty and within a term of 24 hours at the latest, to inform thereof a person's family or his cohabitee or other person with whom he lives in a permanent life community, except if he expressly rejects that.</p> <p>(2) If an attorney at law is detained, the police authority or the court is bound to inform on detention a respective Bar Association immediately and at the latest on the next working day.</p> <p>(3) A social guardianship authority shall be informed about deprivation of liberty if it is necessary to take measures for securing children and other family members to whom the person deprived of liberty is a legal guardian.</p> <p><i>amendment</i></p> <p><i>(2) If an attorney at law is detained, the police authority or the court is bound to inform on detention a respective Bar Association immediately.</i></p>
<p>Article 18 – Production order</p> <p>1 Each Party shall adopt such legislative and other measures as may be</p>	<p>Article 85 paragraph 1 of CPC can be applied.</p> <p>ARTICLE 85</p>

<p>necessary to empower its competent authorities to order:</p> <p>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</p> <p>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.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>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:</p> <p>a the type of communication service used, the technical provisions taken thereto and the period of service;</p> <p>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;</p> <p>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.</p>	<p>(1) The investigating judge may order on his own initiative or upon the motion of the State Attorney that postal, telephone and other communication agencies retain and deliver to him, against a receipt, letters, telegrams and other shipments addressed to the defendant or sent by him if circumstances exist which indicate that it is likely that these shipments can be used as evidence in the proceedings.</p> <p>(2) The shipments shall be opened by the investigating judge in the presence of two witnesses. When opening, care shall be taken not to damage the seals, while the covers and addresses shall be preserved. A record shall be drawn up on the opening.</p> <p>(3) If the interests of the proceedings so allow, the defendant or the addressee may be fully or partially informed of the contents of the shipment, which may be delivered to him as well. If the defendant is absent, the shipment shall be returned to the sender unless this would prejudice the interests of the proceedings.</p> <p>amendment like above</p>
<p>Article 19 – Search and seizure of stored computer data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <p>a a computer system or part of it and computer data stored therein; and</p> <p>b a computer-data storage medium in which computer data may be stored</p> <p style="padding-left: 40px;">in its territory.</p> <p>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</p>	<p>Article 85, 146 paragraph 5, and 147 paragraph 1 and 2 of CPC can also be applied for these purpose.</p> <p>ARTICLE 85</p> <p>(1) The investigating judge may order on his own initiative or upon the motion of the State Attorney that postal, telephone and other communication agencies retain and deliver to him, against a receipt, letters, telegrams and other shipments addressed to the defendant or sent by him if circumstances exist which indicate that it is likely that these shipments can be used as evidence in the proceedings.</p> <p>(2) The shipments shall be opened by the investigating judge in the presence of two witnesses. When opening, care shall be taken not to damage the seals, while the covers and addresses shall be preserved. A record shall be drawn up on the opening.</p>

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

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

- a seize or similarly secure a computer system or part of it or a computer-data storage medium;
- b make and retain a copy of those computer data;
- c maintain the integrity of the relevant stored computer data;
- d render inaccessible or remove those computer data in the accessed computer system.

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

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

(3) If the interests of the proceedings so allow, the defendant or the addressee may be fully or partially informed of the contents of the shipment, which may be delivered to him as well. If the defendant is absent, the shipment shall be returned to the sender unless this would prejudice the interests of the proceedings.

amendment like above

ARTICLE 146

(1) After the indictment has been submitted to the court and up to the closing of the trial, detention may be ordered or vacated only by the ruling rendered by the panel, provided that the opinion of the State Attorney is obtained if the proceedings are conducted upon his request.

(2) Even without motion submitted by parties, the panel is bound to review whether the grounds for detention still exist and to prolong or vacate it by a ruling every month from the moment the last ruling on detention becomes finale, and every two months from the moment the indictment becomes final.

(3) After the indictment is preferred detention may last two years at the longest. If within this period a judgment at first instance fails to be pronounced, detention shall be vacated and a detainee released.

(4) After the judgement at first instance is imposed, detention may last one year at the longest. If within this period a judgement at second instance, by which the judgement at first instance is revised or affirmed, is not rendered, detention shall be vacated and the accused released. If within a term of one year a court at second instance renders a judgement vacating the judgement at first instance, detention may last at the longest for one more year from the day the judgement at second instance is rendered.

(5) An appeal on the ruling referred to in paragraphs 1 and 2 of this Article does not stay the execution of the ruling.

(6) The ruling of the panel by which the motion to order or vacate detention is rejected is not appealable.

amendment like above

ARTICLE 147

(1) The police authority or the court is bound immediately after a person has been deprived of liberty and within a term of 24 hours at the latest, to inform

	<p>thereof a person's family or his cohabitee or other person with whom he lives in a permanent life community, except if he expressly rejects that.</p> <p>(2) If an attorney at law is detained, the police authority or the court is bound to inform on detention a respective Bar Association immediately and at the latest on the next working day.</p> <p>(3) A social guardianship authority shall be informed about deprivation of liberty if it is necessary to take measures for securing children and other family members to whom the person deprived of liberty is a legal guardian.</p> <p>amendment like mentioned</p>
<p>Article 20 – Real-time collection of traffic data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>There are no provisions for this direct purpose.</p>

<p>Article 21 – Interception of content data</p> <p>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:</p> <p>a collect or record through the application of technical means on the territory of that Party, and</p> <p>b compel a service provider, within its existing technical capability:</p> <p> i to collect or record through the application of technical means on the territory of that Party, or</p> <p> 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.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.</p> <p>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.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>For these purposes article 146 paragraph 3,4 and 5, and article 155 can be applied.</p> <p>ARTICLE 146</p> <p>(1) After the indictment has been submitted to the court and up to the closing of the trial, detention may be ordered or vacated only by the ruling rendered by the panel, provided that the opinion of the State Attorney is obtained if the proceedings are conducted upon his request.</p> <p>(2) Even without motion submitted by parties, the panel is bound to review whether the grounds for detention still exist and to prolong or vacate it by a ruling every month from the moment the last ruling on detention becomes finale, and every two months from the moment the indictment becomes final.</p> <p>(3) After the indictment is preferred detention may last two years at the longest. If within this period a judgment at first instance fails to be pronounced, detention shall be vacated and a detainee released.</p> <p>(4) After the judgement at first instance is imposed, detention may last one year at the longest. If within this period a judgement at second instance, by which the judgement at first instance is revised or affirmed, is not rendered, detention shall be vacated and the accused released. If within a term of one year a court at second instance renders a judgement vacating the judgement at first instance, detention may last at the longest for one more year from the day the judgement at second instance is rendered.</p> <p>(5) An appeal on the ruling referred to in paragraphs 1 and 2 of this Article does not stay the execution of the ruling.</p> <p>(6) The ruling of the panel by which the motion to order or vacate detention is rejected is not appealable.</p>
<p>Section 3 – Jurisdiction</p>	
<p>Article 22 – Jurisdiction</p> <p>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:</p> <p>a in its territory; or</p> <p>b on board a ship flying the flag of that Party; or</p> <p>c on board an aircraft registered under the laws of that Party; or</p>	<p>This question is regulated in Chapter 34 of CPC named as “The Procedure for applying of International Legal Assistance and execution of International Contracts in Criminal matters” according to articles 507-515, as well as, the Law on Organization and Jurisdiction of State Authorities for Combating the High – Tech Criminality, according to articles 4 – 11.</p>

<p>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.</p> <p>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.</p> <p>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.</p> <p>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>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.</p>	
<p>Chapter III – International co-operation</p>	
<p>Article 24 – Extradition</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>3 If a Party that makes extradition conditional on the existence of a treaty</p>	<p>This question is regulated in Chapter 35 of CPC named as “Procedure for extradition of accused and sentenced persons” according to articles 516- 532.</p>

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

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

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

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

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

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure

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.

Mutual assistance is provided according to the principles of international legal assistance accepted in our legislative, and above mentioned legal documents.

<p>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.</p> <p>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.</p> <p>5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.</p>	
<p>Article 26 – Spontaneous information</p> <p>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.</p> <p>2 Prior to providing such information, the providing Party may request that it</p>	<p>Our Party accepts the principles connected to spontaneous information as stated in the Convention.</p>

<p>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.</p>	
<p>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</p> <p>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.</p> <p>2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.</p> <p>b The central authorities shall communicate directly with each other;</p> <p>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;</p> <p>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.</p> <p>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.</p> <p>4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or</p> <p>b it considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p> <p>5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its</p>	<p>In those Cases Chapter 34 of CPC is applied.</p>

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

Our legal system accepts the principle of Confidentiality and limitation of use as

<p>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.</p> <p>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:</p> <p>a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or</p> <p>b not used for investigations or proceedings other than those stated in the request.</p> <p>3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.</p> <p>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.</p>	<p>stated in the Convention, so this question is regulated in the article 147, paragraph 4 and 5 of CPC.</p>
<p>Article 29 – Expedited preservation of stored computer data</p> <p>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.</p> <p>2 A request for preservation made under paragraph 1 shall specify:</p> <p>a the authority seeking the preservation;</p> <p>b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;</p> <p>c the stored computer data to be preserved and its relationship to the offence;</p> <p>d any available information identifying the custodian of the stored computer data or the location of the computer system;</p> <p>e the necessity of the preservation; and</p> <p>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</p>	<p>At this point, our legislation does not provide specific regulations for expedited preservation of stored computer data in the sense of article 29 of the Convention.</p>

the stored computer data.

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

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

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

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

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

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

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

Also we do not have provisions for expedited disclosure of data stored and preserved in the sense of article 29.

<p>data to identify that service provider and the path through which the communication was transmitted.</p> <p>2 Disclosure of traffic data under paragraph 1 may only be withheld if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	
<p>Article 31 – Mutual assistance regarding accessing of stored computer data</p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p> <p>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.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <p>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</p> <p>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</p>	<p>Provisions under Chapter 34 of CPC can be used in this case.</p>
<p>Article 32 – Trans-border access to stored computer data with consent or where publicly available</p> <p>A Party may, without the authorisation of another Party:</p> <p>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</p> <p>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.</p>	<p>Provisions under Chapter 34 of CPC can be used in this case.</p>
<p>Article 33 – Mutual assistance in the real-time collection of traffic data</p> <p>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</p>	<p>This kind of assistance is not specifically provided in our legislation.</p>

<p>provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>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.</p>	
<p>Article 34 – Mutual assistance regarding the interception of content data</p> <p>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.</p>	<p>Also, this kind of cooperation is not specifically provided for, in our legislative system.</p>
<p>Article 35 – 24/7 Network</p> <p>1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	
<p>Article 42 – Reservations</p>	<p>Secretariat General on 16 July 2009 - Or. Engl.</p>

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.

In accordance with Articles 24, 27 and 35 of the Convention, Serbia designates as the central authorities in charge for the implementation of the Convention :

Ministry of Interior of the Republic of Serbia
Directorate of Crime Police
Department for the fight against organized crime
Bulevar Mihajla Pupina 2
11070 Novi Beograd

[Note by the Secretariat : Detailed contact information are available on the restricted access part of the Convention Committee on Cybercrime's website on www.coe.int/tcy.]

Period covered: 1/8/2009 -

The preceding statement concerns Article(s) : 24, 27, 35