

CyberCrime@IPA project www.coe.int/cybercrime

Version December 2010

Cybercrime legislation - country profile

MONTENEGRO

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

Tel: +33-3-9021-4506

Directorate General of Human Rights and Legal Affairs

Fax: +33-3-9021-5650

Council of Europe, Strasbourg, France

Email: alexander.seger@coe.int

www.coe.int/cybercrime

| Country: | Montenegro |
|---|--|
| Signature of Convention: | 7/4/2005 (State Union of Serbia and Montenegro is the signatory to the Convention) |
| Ratification/accession: | 3/3/2010 |
| Provisions of the Convention | Corresponding provisions/solutions in national legislation |
| | (pls quote or summarise briefly; pls attach relevant extracts as an appendix) |
| Chapter I – Use of terms | |
| | |
| Article 1 - "Computer system", "computer data", | "service provider". Article 142 of the Criminal Code, paragraphs 17, 18, 19 and 20 |

"traffic data":

For the purposes of this Convention:

- "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;
- "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;
- "service provider" means:
- ability to communicate by means of a computer system, and
- any other entity that processes or stores computer data on behalf of such communication service or users of such service;
- "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

- (1) The territory of Montenegro is deemed to embrace the land territory, seashore and water areas within its borders, as well as air space above it.
- (2) Criminal legislation of Montenegro implies this Code, as well as all other criminal provisions contained in other laws of Montenegro.
- (3) Persons in official capacity are deemed to be:
 - 1) persons who perform official duties in state bodies;
- 2) elected, appointed or designated persons in a state body, a local selfany public or private entity that provides to users of its service the government body or a person who performs on a permanent or temporary basis official duties or official functions in these bodies;
 - 3) persons in an institution, business organization or other entity who are assigned the performance of public authorizations, who decide on rights, obligations or interests of natural and legal persons or on public interest;
 - 4) other persons who perform official duties on the basis of the law, regulations passed on the basis of the law, agreements or arbitration agreements, as well as the persons who are entrusted with performing certain official duties or affairs,
 - 5) military persons, with the exception of provisions of Chapter Thirty Four of this Code.
 - 5a) persons who in a foreign state perform legislative, executive, judicial, or any other public function for the foreign state, persons who perform official duties in an international public organization or persons who perform judicial, prosecutorial or any other function in an international court.
 - (4) Responsible persons are deemed to be owners of a business organisation or other entity, or persons within a business organisation, institution or other entity assigned with (in consideration of his/her function, funds invested or his/her authorizations) a specific scope of affairs in the management of property, production or other trade or in supervision thereof or who are entrusted with the

performance of specific affairs. Responsible persons are also deemed to be persons in official capacity, in the event of criminal offences for which a responsible person is designated as an offender, such offences not being envisaged by this Code in the Chapter dealing with criminal offences against official duties i.e. as criminal offences of a person in official capacity.

- (5) Military persons are deemed to be: professional military person (soldier under contract, officers under contract, non-commissioned officers under contract), person in the reserve army (reserve soldier, reserve officer, reserve non-commissioned officer), civilians performing a specific military duty and persons who are subject to military duty in the emergency situations.
- (6) When a person in official capacity, a responsible person or a military person is designated as a perpetrator of specific criminal offences, persons referred to in paras. 3, 4 and 5 of this Article may be perpetrators of these acts, unless the elements of an individual offence or an individual regulation imply that the offender may be solely someone of these persons.
- (7) Children are deemed to be persons who have not reached the age of fourteen.
- (8) Juveniles are deemed to be persons who have reached the age of fourteen, but not the age of eighteen.
- (9) Underage persons are deemed to be persons who have not reached the age of eighteen.
- (10) Offenders are deemed to be perpetrators, co-offenders, inciters and aiders.
- (11) Force is deemed to be the use of hypnosis or overpowering agents with the purpose of bringing someone against his/her will to the state of unconsciousness or inability to give resistance.
- (12) Elections are deemed to be the elections for the Parliament of Montenegro, President of Montenegro, local self-government bodies and other elections called

for and conducted on the basis of the Constitution and law.

- (13) Referendum is deemed to be voting of citizens where they decide on the issues specified by the Constitution and law.
- (14) Narcotics are deemed to be substances and preparations declared by regulations founded on law to be narcotics.
- (15) Movable articles are deemed to include generated or collected energy for production of light, heat or movement, telephone impulses, as well as computer data and a computer program.
- (16) Computer system is every device, or a group of interconnected or conditioned devices, one or several of which, depending on the programme, perform automatic data processing
- (17) Computer data are deemed to be presentations of facts, data or concepts in the form that is convenient for processing in a computer system, including the programmes used by computer system for its functions.
- (18) Computer programs are deemed to be sets of ordered computer data on the basis of which computers perform their function.
- (19) Computer viruses are computer programs that threaten or change the function of the computer system and change, threaten or use computer data without authorization.
- (20) Data on computer traffic are all computer data generated by computer systems that form a chain of communication between two communicating computer systems, including them.
- (21) Protected natural assets are deemed also to be assets that, under regulations on protection of natural assets, enjoy previous protection.
- (22) Cultural assets are deemed also to be assets that, under regulations on

protection of cultural assets, enjoy previous protection, as well as a part of cultural asset and protected environment of an immovable cultural asset.

- (23) Money means both metal coins or paper money or money made of some other material that is in circulation in Montenegro or a foreign country under law.
- (24) Value symbols include foreign value symbols.
- (25) Motor vehicle is deemed to be every transportation means with a motor drive used in the land, water and air transportation.
- (26) Documents are deemed to be all objects that are suitable for or designated to serve as an evidence of a specific fact of relevance for legal relations, as well as a computer data.
- (27) Files, letters, parcels and documents may also be in an electronic form.
- (28) Families or family communities include former spouses, cognates and fully adopted relatives in a direct line without limitation, whereas in a collateral line ending with the fourth degree, family or family communities include openly adopted relatives, relatives by marriage ending with the second degree, persons who live in the same household and individuals that have a joint child or a child is on the way, although they have never lived in the same household.
- (29) The expression "shall not be punished" means that in the case there is no criminal offence.
- (30) When an imperfective verb is used to designate the action of a criminal offence, it shall be deemed that the offence is committed if the action is done once or several times.

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

Section 28 of the Criminal Code of Montenegro "Criminal Acts against

Each Party shall adopt such legislative and other measures as may be Safety of Computer Data" necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer Article 355 - Accessing protected computer and computer network 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.

without authorization

- (1) Anyone who, violating the protection measures, connects into a computer or a computer network without authorization, shall be liable to a fine or imprisonment for a term not exceeding one year.
- (2) Punishment as of paragraph 1 of this Article shall be imposed on anyone committing an unauthorized interception of computer data.
- (3) Anyone who uses a datum obtained in the manner envisaged by Paragraph 1 and 2 of this Article, shall be liable to a fine or imprisonment for a term not exceeding three years.
- (4) If due to acts referred to in Paragraph 3 of this Article, severe consequences occurred for another person, the offender shall be punished by imprisonment for a term of six months to five years. This article is deleted

Article 353 - Unauthorized Access to Computer System

- (1) Anyone who without authorization accesses a computer system as a whole or a part of it shall be punished by a fine or imprisonment not exceeding one year.
- (2) If the offender committed the offence referred to in para 1 of this Article by violating the measures of protection of a computer system he shall be punished by a fine or imprisonment of up to three years.
- (3) The punishment referred to in para 2 of this Article shall also be imposed on a person who intercepts computer data without authorization, regardless of the manner of transfer of computer data, which are not of public nature, to the computer system, from the computer system or within the computer system, including the electro-magnetic emission/
- (4) Anyone who uses the data obtained in the manner provided for in paras 1, 2 and 3 of this Article, shall be punished by a fine or imprisonment not exceeding three years.
- (5) Where the offence referred to in paragraph 4 of this Article has severe

consequences, the offender shall be punished by an imprisonment sentence of six months to five years.

Article 3 – Illegal interception

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

TITLE TWENTY EIGHT CRIMINAL OFFENCES AGAINST SAFETY OF COMPUTER DATA

Article 349 - Damaging Computer Data and Programs

- (1) Anyone who without authorization deletes, alters, damages, conceals or in any other manner makes useless a computer datum or a program, shall be punished by a fine or imprisonment not exceeding one year.
- (2) Where through an offence referred to in paragraph 1 of this Article damage exceeding the amount of three thousand euro was caused, the offender shall be punished by an imprisonment sentence of three months to three years.
- (3) Where through an offence referred to in paragraph 1 of this Article damage exceeding the amount of thirty thousand euro was caused, the offender shall be punished by an imprisonment sentence of three months to five years.
- (4) If devices and means used for committing a criminal offence referred to in paras. 1, 2 and 3 of this Article are the possession of the offender, they shall be seized.

Article 350 - Obstructing Computer System

- (1) Anyone who enters, destroys, deletes, alters, damages, conceals or in any other manner makes useless a computer datum or a computer system in the intention to obstruct the operation of the computer system, shall be punished by a fine or an imprisonment sentence of up to three years.
- (2) If the offence referred to in para 1 of this Article is committed against data or programmes which are significant for state bodies, public services, institutions, business organisations or other entities, the offender shall be punished by an imprisonment sentence of one to eight years.

(3) If devices and means used for committing a criminal offence referred to in paras. 1 and 2 of this Article are the possession of the offender, they shall be seized.

Article 351 - Producing and Planting Computer Viruses

- (1) Anyone who makes a computer virus with the intention of planting it into another's computer system shall be punished by a fine or imprisonment not exceeding one year.
- (2) If the offender planted a computer virus into another's computer system and thereby caused damage, s/he shall be punished by a fine or imprisonment not exceeding two years.
- (3) The device and means used for committing a criminal offence referred to in paras. 1 and 2 of this Article shall be seized.

Article 352 - Computer Fraud

- (1) Anyone who enters, changes, deletes, fails to enter a correct datum or in some other manner conceals or falsely presents a piece of computer data or obstructs in any other way the operation of a computer system and thereby influences the result of electronic processing, transfer of data and operations of a computer system with the intention of obtaining unlawful material benefit for him/herself or for another and thereby causes property damage to another, shall be punished by an imprisonment sentence of six months to five years.
- (2) Where through an offence referred to in paragraph 1 of this Article material benefit was acquired exceeding the amount of three thousand euro, the offender shall be punished by an imprisonment sentence of two to ten years.
- (3) Where through an offence referred to in paragraph 1 of this Article, material benefit was acquired exceeding the amount of thirty thousand euro, the offender shall be punished by an imprisonment sentence of two to twelve years.
- (4) Where an offence referred to in paragraph 1 of this Article was committed only with the intention to cause damage to another person, the offender shall be

punished by a fine or imprisonment sentence not exceeding two years.

Article 353 - Unauthorized Access to Computer System

- (1) Anyone who without authorization accesses a computer system as a whole or a part of it shall be punished by a fine or imprisonment not exceeding one year.
- (2) If the offender committed the offence referred to in para 1 of this Article by violating the measures of protection of a computer system he shall be punished by a fine or imprisonment of up to three years.
- (3) The punishment referred to in para 2 of this Article shall also be imposed on a person who intercepts computer data without authorization, regardless of the manner of transfer of computer data, which are not of public nature, to the computer system, from the computer system or within the computer system, including the electro-magnetic emission/
- (4) Anyone who uses the data obtained in the manner provided for in paras 1, 2 and 3 of this Article, shall be punished by a fine or imprisonment not exceeding three years.
- (5) Where the offence referred to in paragraph 4 of this Article has severe consequences, the offender shall be punished by an imprisonment sentence of six months to five years.

Article 354 - Abuse of devices and programmes

- (1) Anyone who produces, sells, procures in the aim to use, imports, distributes and in some other way provides:
- a. Devices and computer programmes projected or adapted primarily for the purpose of committing an offence referred to in Articles 349 to 353 of this Code
- b. Computer code or similar data that can be used for accessing a computer system as a whole or a part of it with the intention to use it for the purpose of committing an offence referred to in Articles 349 to 353 of this Code.

| | (2) Anyone who possesses any means referred to in para 1 of this Article and intends to use them for committing a criminal offence referred to in Articles 349 to 353 of this Code, shall be punished by imprisonment of up to one year | | | |
|--|---|--|--|--|
| 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. | Accessing Protected Computer and Computer Network without Authorization | | | |
| | Article 355 -deleted- | | | |
| | Preventing and Limiting Access to Public Computer Networks | | | |
| | Article 356 -deleted- | | | |
| | Section 28 of the Criminal Code of Montenegro "Criminal Acts against Safety of Computer Data" | | | |
| | Article 349 - Damaging Computer Data and Programs | | | |
| | (1) Anyone who without authorization deletes, alters, damages, conceals or in any other manner makes useless a computer datum or a program, shall be punished by a fine or imprisonment not exceeding one year. | | | |
| | (2) Where through an offence referred to in paragraph 1 of this Article damage exceeding the amount of three thousand euro was caused, the offender shall be punished by an imprisonment sentence of three months to three years. | | | |
| | (3) Where through an offence referred to in paragraph 1 of this Article damage exceeding the amount of thirty thousand euro was caused, the offender shall be punished by an imprisonment sentence of three months to five years. | | | |
| | (4) If devices and means used for committing a criminal offence referred to in paras. 1, 2 and 3 of this Article are the possession of the offender, they shall be | | | |

seized.

Article 351 - Producing and Planting Computer Viruses

- (1) Anyone who makes a computer virus with the intention of planting it into another's computer system shall be punished by a fine or imprisonment not exceeding one year.
- (2) If the offender planted a computer virus into another's computer system and thereby caused damage, s/he shall be punished by a fine or imprisonment not exceeding two years.
- (3) The device and means used for committing a criminal offence referred to in paras. 1 and 2 of this Article shall be seized.

Article 352 - Computer Fraud

- (1) Anyone who enters, changes, deletes, fails to enter a correct datum or in some other manner conceals or falsely presents a piece of computer data or obstructs in any other way the operation of a computer system and thereby influences the result of electronic processing, transfer of data and operations of a computer system with the intention of obtaining unlawful material benefit for him/herself or for another and thereby causes property damage to another, shall be punished by an imprisonment sentence of six months to five years.
- (2) Where through an offence referred to in paragraph 1 of this Article material benefit was acquired exceeding the amount of three thousand euro, the offender shall be punished by an imprisonment sentence of two to ten years.
- (3) Where through an offence referred to in paragraph 1 of this Article, material benefit was acquired exceeding the amount of thirty thousand euro, the offender shall be punished by an imprisonment sentence of two to twelve years.
- (4) Where an offence referred to in paragraph 1 of this Article was committed only with the intention to cause damage to another person, the offender shall be

punished by a fine or imprisonment sentence not exceeding two 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

Section 28 of the Criminal Code of Montenegro "Criminal Acts against Safety of Computer Data"

Article 350 - Obstructing Computer System

- (4) Anyone who enters, destroys, deletes, alters, damages, conceals or in any other manner makes useless a computer datum or a computer system in the intention to obstruct the operation of the computer system, shall be punished by a fine or an imprisonment sentence of up to three years.
- (5) If the offence referred to in para 1 of this Article is committed against data or programmes which are significant for state bodies, public services, institutions, business organisations or other entities, the offender shall be punished by an imprisonment sentence of one to eight years.
- (6) If devices and means used for committing a criminal offence referred to in paras. 1 and 2 of this Article are the possession of the offender, they shall be seized.

Article 351 - Producing and Planting Computer Viruses

- (1) Anyone who makes a computer virus with the intention of planting it into another's computer system shall be punished by a fine or imprisonment not exceeding one year.
- (2) If the offender planted a computer virus into another's computer system and thereby caused damage, s/he shall be punished by a fine or imprisonment not exceeding two years.
- (3) The device and means used for committing a criminal offence referred to in paras. 1 and 2 of this Article shall be seized.

Article 352 - Computer Fraud

(1) Anyone who enters, changes, deletes, fails to enter a correct datum or in

some other manner conceals or falsely presents a piece of computer data or obstructs in any other way the operation of a computer system and thereby influences the result of electronic processing, transfer of data and operations of a computer system with the intention of obtaining unlawful material benefit for him/herself or for another and thereby causes property damage to another, shall be punished by an imprisonment sentence of six months to five years.

- (2) Where through an offence referred to in paragraph 1 of this Article material benefit was acquired exceeding the amount of three thousand euro, the offender shall be punished by an imprisonment sentence of two to ten years.
- (3) Where through an offence referred to in paragraph 1 of this Article, material benefit was acquired exceeding the amount of thirty thousand euro, the offender shall be punished by an imprisonment sentence of two to twelve years.
- (4) Where an offence referred to in paragraph 1 of this Article was committed only with the intention to cause damage to another person, the offender shall be punished by a fine or imprisonment sentence not exceeding two years.

Article 354 - Abuse of devices and programmes

- (3) Anyone who produces, sells, procures in the aim to use, imports, distributes and in some other way provides:
- a. Devices and computer programmes projected or adapted primarily for the purpose of committing an offence referred to in Articles 349 to 353 of this Code
- b. Computer code or similar data that can be used for accessing a computer system as a whole or a part of it with the intention to use it for the purpose of committing an offence referred to in Articles 349 to 353 of this Code.
- (4) Anyone who possesses any means referred to in para 1 of this Article and intends to use them for committing a criminal offence referred to in Articles 349 to 353 of this Code, shall be punished by imprisonment of up to one year

Article 6 - Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be Safety of Computer Data"

Section 28 of the Criminal Code of Montenegro "Criminal Acts against Safety of Computer Data"

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:
- 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;
- 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
- the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
- 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
- 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Article 351 - Producing and Planting Computer Viruses

- (1) Anyone who makes a computer virus with the intention of planting it into another's computer system shall be punished by a fine or imprisonment not exceeding one year.
- (2) If the offender planted a computer virus into another's computer system and thereby caused damage, s/he shall be punished by a fine or imprisonment not exceeding two years.
- (3) The device and means used for committing a criminal offence referred to in paras. 1 and 2 of this Article shall be seized.

Title 2 - Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be Safety of Computer Data" 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,

Section 28 of the Criminal Code of Montenegro "Criminal Acts against

Article 352 - Computer Fraud

(1) Anyone who enters, changes, deletes, fails to enter a correct datum or in some other manner conceals or falsely presents a piece of computer data or

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.

obstructs in any other way the operation of a computer system and thereby influences the result of electronic processing, transfer of data and operations of a computer system with the intention of obtaining unlawful material benefit for him/herself or for another and thereby causes property damage to another, shall be punished by an imprisonment sentence of six months to five years.

- (2) Where through an offence referred to in paragraph 1 of this Article material benefit was acquired exceeding the amount of three thousand euro, the offender shall be punished by an imprisonment sentence of two to ten years.
- (3) Where through an offence referred to in paragraph 1 of this Article, material benefit was acquired exceeding the amount of thirty thousand euro, the offender shall be punished by an imprisonment sentence of two to twelve years.
- (4) Where an offence referred to in paragraph 1 of this Article was committed only with the intention to cause damage to another person, the offender shall be punished by a fine or imprisonment sentence not exceeding two years.

Article 8 - Computer-related fraud

Each Party shall adopt such legislative and other measures as may be Safety of Computer Data" 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:

- any input, alteration, deletion or suppression of computer data;
- 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.

Section 28 of the Criminal Code of Montenegro "Criminal Acts against

Article 352 - Computer Fraud

- (1) Anyone who enters, changes, deletes, fails to enter a correct datum or in some other manner conceals or falsely presents a piece of computer data or obstructs in any other way the operation of a computer system and thereby influences the result of electronic processing, transfer of data and operations of a computer system with the intention of obtaining unlawful material benefit for him/herself or for another and thereby causes property damage to another, shall be punished by an imprisonment sentence of six months to five years.
- (2) Where through an offence referred to in paragraph 1 of this Article material benefit was acquired exceeding the amount of three thousand euro, the offender shall be punished by an imprisonment sentence of two to ten years.
- (3) Where through an offence referred to in paragraph 1 of this Article, material

benefit was acquired exceeding the amount of thirty thousand euro, the offender shall be punished by an imprisonment sentence of two to twelve years.

(4) Where an offence referred to in paragraph 1 of this Article was committed only with the intention to cause damage to another person, the offender shall be punished by a fine or imprisonment sentence not exceeding two years.

Title 3 - Content-related offences

Article 9 – Offences related to child pornography

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

 Article 211 Pientering B.
 - producing child pornography for the purpose of its distribution through a computer system;
 - offering or making available child pornography through a computer system;
 - distributing or transmitting child pornography through a computer system;
 - d procuring child pornography through a computer system for oneself or for another person;
 - 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 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 agelimit, 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.

Section 28 of the Criminal Code of Montenegro "Criminal Acts against Safety of Computer Data"

Article 211 - Displaying Pornographic Material to Children and Producing and Possessing Children Pornography

- (1) Anyone who sells or displays to a child or by public displaying or in some other manner makes available text, pictures, audio-visual or other objects of pornographic content or displays to a child any pornographic show, shall be punished by a fine or an imprisonment sentence not exceeding six months.
- (2) Anyone who uses a juvenile to produce pictures, audio-visual or other objects of pornographic content or for a pornographic show, shall be punished by an imprisonment sentence of six months to five years.
- (3) Anyone who procures, sells, shows, attends a show, publicly exhibits or in electronic or some other manner makes available pictures, audio-visual or other objects of pornographic content resulting from acts referred to in paragraph 2 of this Article or who possesses such objects shall be punished by an imprisonment sentence not exceeding two years.
- (4) If the offence referred to in paragraphs 2 and 3 of this Article is committed against a child, the punishment shall be from one to eight years for the offence referred to in paragraph 2 and from six months to five years for the offence referred to in paragraph 3.
- (5) If the offence referred to in paragraph 2 of this Article is committed by using force or threat, the offender shall be punished by imprisonment of two to ten



- (6) the person who possesses objects of pornographic contents shall not be punished for the offence referred to in paragraph 3 of this Article if the senior iuvenile that is shown in the contents gave its consent, and the person keeps such objects solely for his own use.
- (7) Objects referred to in paras. 1 to 3 of this Article shall be seized and destroyed.

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

related rights

- 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.
- 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.
- 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

Article 10 - Offences related to infringements of copyright and Section 21 of the Criminal Code of Montenegro "Criminal Acts against Author's, Inventor's and Related Rights"

Article 233 - Violation of Moral Rights of Authors and Performers

- (1) Anyone who in his/her own name or in the name of another person wholly or partially publicizes, releases into circulation copies of someone else's copyrighted work or performance or otherwise publicly discloses someone else's copyrighted work or performance, shall be punished by a fine or an imprisonment sentence not exceeding three years.
- (2) Anyone who without a permit of the author changes or re-makes someone else's copyrighted work or recorded performance shall be punished by a fine or an imprisonment sentence not exceeding one year.
- (3) Anyone who releases into circulation copies of someone else's copyrighted work or performance in a manner which is insulting for the author or performer's honour and reputation, shall be punished by a fine or an imprisonment sentence not exceeding six months.
- (4) Objects of the criminal offence and objects that were used for or intended for the commission of a criminal offence referred to in paras. 1 to 3 of this Article shall be seized and objects of the criminal offence shall be destroyed.

| international instruments referred to in paragraphs 1 and 2 of this article. | (5) Prosecution for an offence referred to in paragraph 3 of this Article shall be undertaken upon a personal action at law. |
|--|---|
| | Article 234 -Unauthorized Use of Copyrighted Works or Objects of Related Rights |
| | (1) Whoever publicizes, records, duplicates or otherwise publicly discloses or makes available, in whole or in part, a copyrighted work, performance, phonogram, videogram, show or database, shall be punished by an imprisonment sentence not exceeding three years. |
| | (2) The sentence referred to in paragraph 1 of this Article shall also imposed on anyone who releases into circulation, or with the intention of releasing into circulation, keeps unauthorizedly duplicated or unauthorizedly released into circulation copies of copyrighted works, performances, phonograms, videograms, shows, computer programs or databases. |
| | (3) Where an offence referred to in paras. 1 and 2 of this Article, was committed with the intention of acquiring material benefit for him/herself or another, the offender shall be punished by an imprisonment sentence from three months to five years. |
| | (4) Objects of the criminal offence and objects that were used for or intended for the commission of the criminal offence referred to in paras. 1 and 2 of this Article shall be seized, and objects of the criminal offence shall be destroyed. |
| | Article 235 - Unauthorized Circumvention of Protection Measures Intended for the Prevention of Violations of Copyright and Related Rights and Information on the Right |
| | (1) Anyone who produces, imports, releases into circulation, sells, leases, advertises in the interest of sale or leases or keeps for commercial purposes devices or means whose basic or main purpose is removal, circumvention or thwarting of technological measures intended for the prevention of violations of copyright and related rights or who uses such devices or means in the interest of violating copyright or related rights, shall be punished by fine or imprisonment |

not exceeding three years.

(2) Objects of the criminal offence and objects that were used for or intended for the commission of criminal offence referred to in paragraph 1 of this Article shall be seized, and objects of the criminal offence shall be destroyed.

Article 236 - Unauthorized Removal or Modification of Electronic Information on Copyright and Related Rights

- (1) Whoever without authorization removes or alters an electronic information on copyright and related rights, or releases into circulation, imports, broadcasts or otherwise publicly discloses or makes available a copyrighted work or object of related legal protection, from which an electronic information on the rights was unauthorizedly removed or modified, shall be punished by fine or imprisonment sentence not exceeding three years.
- (2) Objects of the criminal offence and objects that were used for or intended for the commission of criminal offences referred to in paragraph 1 of this Article shall be seized, and objects of the criminal offence shall be destroyed.

Article 237 - Unauthorized Use of Someone Else's Patent

- (1) Anyone who unauthorizedly produces, imports, exports, offers in view of releasing into circulation, releases into circulation, stores or uses in commercial transactions a product or procedure protected by patent, shall be punished by fine or imprisonment sentence not exceeding three years.
- (2) Where material benefit was obtained through an offence referred to in paragraph 1 of this Article or damage caused in an amount that exceeds thirty thousand euro, the offender shall be punished by an imprisonment from one to eight years.
- (3) Whoever unauthorizedly publicizes or otherwise makes available the essence of someone else's reported invention before the invention was made public in the manner laid down by law, shall be punished by a fine or imprisonment sentence not exceeding two years.

- (4) Whoever unauthorizedly files a patent application or does not indicate the inventor in the application or indicates him/her falsely, shall be punished by an imprisonment sentence from six months to five years.
- (5) Objects of the criminal offence and objects that were used for or intended for the commission of a criminal offence referred to paras. 1 and 3 of this Article shall be seized and objects of the criminal offence shall be destroyed.

Article 238 - Unauthorized Use of Someone Else's Design

- (1) Whoever unauthorizedly uses, wholly or in part, someone else's registered or protected product design on their traded product, shall be punished by a fine or imprisonment sentence not exceeding three years.
- (2) Whoever unauthorizedly publicizes or otherwise makes available to the public the subject matter of an application of someone else's design before it was publicized in the manner laid down by law, shall be punished by a fine or imprisonment sentence not exceeding one year.
- (3) Objects of the criminal offence and objects that were used for or intended for the commission of criminal offences referred to in paragraph 1 of this Article shall be seized, and objects of the criminal offence shall be destroyed.

Title 5 - Ancillary liability and sanctions

Article 11 - Attempt and aiding or abetting

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
- 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.
- 3 Each Party may reserve the right not to apply, in whole or in part,

| | _ | _ | | |
|-----------|---|----------|------|----------|
| paragraph | , | \cap t | thic | articla |
| Daragraph | _ | OI. | uiio | ai dele. |

Article 12 - Corporate liability

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
 - a a power of representation of the legal person;
 - b an authority to take decisions on behalf of the legal person;
 - an authority to exercise control within the legal person.
- 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
- 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
- 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 - Sanctions and measures

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
- 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

The Law on Liability of Legal Persons for Criminal Acts (Official Gazette of the Republic of Montenegro no. 2/07 and 13/07 from 2006)

TITLE TWENTY EIGHT CRIMINAL OFFENCES AGAINST SAFETY OF COMPUTER DATA

Article 349 - Damaging Computer Data and Programs

- (1) Anyone who without authorization deletes, alters, damages, conceals or in any other manner makes useless a computer datum or a program, shall be punished by a fine or imprisonment not exceeding one year.
- (2) Where through an offence referred to in paragraph 1 of this Article damage exceeding the amount of three thousand euro was caused, the offender shall be punished by an imprisonment sentence of three months to three years.
- (3) Where through an offence referred to in paragraph 1 of this Article damage exceeding the amount of thirty thousand euro was caused, the offender shall be punished by an imprisonment sentence of three months to five years.

(4) If devices and means used for committing a criminal offence referred to in paras. 1, 2 and 3 of this Article are the possession of the offender, they shall be seized.

Article 350 - Obstructing Computer System

- (7) Anyone who enters, destroys, deletes, alters, damages, conceals or in any other manner makes useless a computer datum or a computer system in the intention to obstruct the operation of the computer system, shall be punished by a fine or an imprisonment sentence of up to three years.
- (8) If the offence referred to in para 1 of this Article is committed against data or programmes which are significant for state bodies, public services, institutions, business organisations or other entities, the offender shall be punished by an imprisonment sentence of one to eight years.
- (9) If devices and means used for committing a criminal offence referred to in paras. 1 and 2 of this Article are the possession of the offender, they shall be seized.

Article 351 - Producing and Planting Computer Viruses

- (1) Anyone who makes a computer virus with the intention of planting it into another's computer system shall be punished by a fine or imprisonment not exceeding one year.
- (2) If the offender planted a computer virus into another's computer system and thereby caused damage, s/he shall be punished by a fine or imprisonment not exceeding two years.
- (3) The device and means used for committing a criminal offence referred to in paras. 1 and 2 of this Article shall be seized.

Article 352 - Computer Fraud

(1) Anyone who enters, changes, deletes, fails to enter a correct datum or in some other manner conceals or falsely presents a piece of computer data or

obstructs in any other way the operation of a computer system and thereby influences the result of electronic processing, transfer of data and operations of a computer system with the intention of obtaining unlawful material benefit for him/herself or for another and thereby causes property damage to another, shall be punished by an imprisonment sentence of six months to five years.

- (2) Where through an offence referred to in paragraph 1 of this Article material benefit was acquired exceeding the amount of three thousand euro, the offender shall be punished by an imprisonment sentence of two to ten years.
- (3) Where through an offence referred to in paragraph 1 of this Article, material benefit was acquired exceeding the amount of thirty thousand euro, the offender shall be punished by an imprisonment sentence of two to twelve years.
- (4) Where an offence referred to in paragraph 1 of this Article was committed only with the intention to cause damage to another person, the offender shall be punished by a fine or imprisonment sentence not exceeding two years.

Article 353 - Unauthorized Access to Computer System

- (6) Anyone who without authorization accesses a computer system as a whole or a part of it shall be punished by a fine or imprisonment not exceeding one year.
- (7) If the offender committed the offence referred to in para 1 of this Article by violating the measures of protection of a computer system he shall be punished by a fine or imprisonment of up to three years.
- (8) The punishment referred to in para 2 of this Article shall also be imposed on a person who intercepts computer data without authorization, regardless of the manner of transfer of computer data, which are not of public nature, to the computer system, from the computer system or within the computer system, including the electro-magnetic emission/
- (9) Anyone who uses the data obtained in the manner provided for in paras 1, 2 and 3 of this Article, shall be punished by a fine or imprisonment not exceeding three years.

(10) Where the offence referred to in paragraph 4 of this Article has severe consequences, the offender shall be punished by an imprisonment sentence of six months to five years.

Article 354 - Abuse of devices and programmes

- (5) Anyone who produces, sells, procures in the aim to use, imports, distributes and in some other way provides:
- a. Devices and computer programmes projected or adapted primarily for the purpose of committing an offence referred to in Articles 349 to 353 of this Code
- b. Computer code or similar data that can be used for accessing a computer system as a whole or a part of it with the intention to use it for the purpose of committing an offence referred to in Articles 349 to 353 of this Code.
- (6) Anyone who possesses any means referred to in para 1 of this Article and intends to use them for committing a criminal offence referred to in Articles 349 to 353 of this Code, shall be punished by imprisonment of up to one year

Accessing Protected Computer and Computer Network without Authorization
Article 355

-deleted-

Preventing and Limiting Access to Public Computer Networks Article 356 -deleted-

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

Criminal Procedure Code, Articles 76, 83 and 86

Article 75 - Reasons for Search of Dwellings, Other Premises, Movable Articles and Persons

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;
- other criminal offences committed by means of a computer system; and
- c the collection of evidence in electronic form of a criminal offence.
- 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
- b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
 - i is being operated for the benefit of a closed group of users, and
 - ii does not employ public communications networks and is not connected with another computer system, whether public or private,

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

- (1) Search of dwelling and other premises of the accused or other persons as well as their movable articles outside the dwelling may be carried out if grounds for suspicion exist that in the course of search the offender would be captured or that traces of the criminal offence or objects relevant to the criminal proceedings would be found.
- (2) The search of movable articles within the meaning of paragraph 1 of this Article shall include the search of computers and similar devices for automatic data processing which are connected to the computer. Upon the request of the court, the person using a computer shall enable access to the computer and to removable storage used for storing information relative to the object of the search (discs, USB flash discs, USB hard discs, floppy disks, tapes and alike), as well as give necessary information on the use of the computer. Persons who refuse to do so although reasons referred to in Article 111 of this Code do not exist may be punished in compliance with Article 85 paragraph 3 of this Code.
- (3) Search of persons may be carried out if grounds for suspicion exist that in the course of search traces and objects relevant to the criminal proceedings would be found.

Article 76 - Search Warrant and Request for a Search Warrant

- (1) A search warrant shall be issued by the court at the request of the State Prosecutor or at the request of an authorized police officer granted authorization by the State Prosecutor, and it shall be enforced by the police.
- (2) A request for the issuance of a search warrant shall be submitted in writing, and only exceptionally orally in line with Article 78 of the present Code.

Article 77 -Contents of the Request for a Search Warrant

The request for issuing a search warrant shall contain:

- 1) the name of the applicant,
- 2) the name of the court to which the request is addressed,
- 3) facts indicating the likelihood that reasons for search exist referred to in Article 75 of the present Code,

- 4) the first and the last name, and, if necessary, a description of the person to be apprehended during the search of dwellings or other premises, or expected traces and a description of objects that should be found by the search,
- 5) the designation of the location of the search, by indicating the address, information about the owner or the person in possession of the objects, dwellings or other premises and any other information of importance to establish the identity, and
- 6) signature of the applicant.

Article 78 - Verbal Request for a Search Warrant

- (1) A verbal request for issuing a search warrant may be filed when risk of delay exists.
- (2) The request from paragraph 1 of this Article may be communicated to the investigating judge also by telephone, radio or other means of electronic communication.
- (3) When a verbal request for issuing a search warrant has been submitted, the investigating judge shall record the further course of conversation. If a voice recording device has been used or stenographic records kept, a transcription thereof shall be made within 24 hours, the identity of which shall be certified and kept with the original records.

Article 79 - Search Warrant

- (1) When the investigating judge receives the request for issuing a search warrant, if s/he agrees with the request, s/he shall immediately issue a search warrant containing:
- 1) the information provided for in Article 77 of the present Code;
- 2) that the search will be conducted by the police;
- 3) an instruction that the search is being done in accordance with Article 80 of the present Code;
- 4) signature of the judge and the official stamp of the court.
- (2) If the investigating judge determines that the request for issuing a search warrant is not justified, s/he shall immediately request the panel referred to in Article 24, paragraph 7 of the present Code to decide on the request. The panel

shall make a decision within 24 hours.

Article 80 - Search Upon a Court Order

- (1) Before the commencement of the search, the search warrant shall be given to the person to be searched or whose premises are to be searched. Before the search, the persons against whom the search warrant has been issued shall be asked to voluntarily hand over the wanted person or objects. Those persons shall be instructed that they are entitled to retain a lawyer i.e. a defense attorney who may be present during the search. If a person against whom a search warrant has been issued demands the presence of a lawyer or defense attorney, the commencement of the search shall be postponed until his/her arrival, but for no more than two hours.
- (2) The search may commence without previously presenting a warrant or without a previous invitation to hand over the person or objects and without an instruction on the right to a defense attorney or lawyer, if it is necessary in order to prevent a criminal offence from being committed, for the purpose of outright capture of a criminal offender, saving of persons and property or if the search is to be carried out in public premises.
- (3) The search shall be carried out by day from 6:00^h until 21:00^h. The search may be carried out by night as well, if it was commenced during the day and was not completed or if it was explicitly ordered so by the court because of risk of delay or if reasons referred to in Article 83 paragraph 1 of the present Code exist.

Article 82 - Seizure of Other Objects by Virtue of a Search Warrant

- (1) If a search of a dwelling or a person reveals objects that are unrelated to the criminal offence for which the search was ordered, but indicate the commission of another criminal offence that is prosecuted ex officio, they shall be described in the record and seized, and a receipt confirming seizure shall be issued immediately.
- (2) If the competent Public Prosecutor was not present during the search, s/he shall immediately be informed about the discovery of objects referred to in

paragraph 1 of this Article in view of initiating criminal proceedings. These objects shall be returned immediately if the Public Prosecutor establishes that there are no grounds to initiate criminal proceedings and if no other legal grounds for the seizure of these objects exist.

(3) If certain objects are seized during the search of computers and similar devices for automatic data processing, they shall be immediately returned to their users, if they are not needed for conducting the procedure. Personal data obtained during the search may be used only for the purpose of conducting criminal proceedings and shall be erased as soon as that purpose ceases.

Article 83 - Entering Another Person's Dwellings without a Search Warrant and Searching

- (1) An authorized police officer may enter another person's dwelling or other premises without a search warrant and, if necessary, carry out the search, provided that the tenant so requires or if it is necessary or for the purpose of preventing the commission of a criminal offence or outright capturing a criminal offender or for the purpose of saving people and property.
- (2) The tenant, if present, shall have the right to object to the procedure of the authorized police officer referred to in paragraph 1 of this Article. The authorized police officer shall inform the tenant about this right and shall include his/her objections in the receipt on entering the dwelling or in the search record.
- (3) In case referred to in paragraph 1 of this Article, if another person's dwelling was only entered without search, the tenant shall be issued a receipt stating the reason for entering the dwelling or other premises as well as the tenant's objections. If search was also carried out in another person's dwelling or other premises, the procedure shall be the one referred to in Article 81, paras. 3, 7 and 8 and Article 82, paragraph 1 of the present Code.
- (4) A search may be carried out without the presence of witnesses if it is not possible to arrange their presence immediately, and risk of delay exists. The reasons for the search without the presence of witnesses shall be specified in a record.

- (5) Authorized police employees may, without a search warrant and without the presence of witnesses, carry out a search of persons when enforcing a warrant on compulsory apprehension or when depriving of liberty, if suspicion exists that the person owns weapons or dangerous tools, or if suspicion exists that the person would reject, hide or destroy the objects that need to be taken from him/her as evidence in a criminal procedure.
- (6) If there are grounds for suspicion that criminal offence was committed that is prosecuted by virtue of office, authorized police employees may, without a court warrant and without the presence of witnesses, carry out the search of transport means, passengers, luggage and other movable objects, with the exception of things referred to in Article 75 paragraph 2 of the present Code.
- (7) When conducting a search without a search warrant, authorized police officers shall immediately submit thereon a report to the investigative judge.

Article 84 - Legally Invalid Evidence

If the search was conducted in contravention to the provisions of Article 76, Article 80 paragraph 1, Article 81 paragraph 3 and Article 83 of the present Code, search records and evidence collected during the search may not be used as evidence in the course of criminal procedure.

Article 85 - Seizure of Objects and Material Benefit

- (1) Objects which have to be seized under the Criminal Code or which may be used as evidence in criminal proceedings, shall, upon the proposal of a Public Prosecutor, and by way of a court ruling, be seized and delivered for safekeeping to the court or their safekeeping shall be secured in another way.
- (2) The ruling on the seizure of objects shall contain:
- 1) the name of the court issuing the ruling,
- 2) legal grounds for the seizure of objects,

- 3) indication and description of objects that are to be seized,
- 4) forename and family name of the person from whom the object is seized and the place at or in which a certain object should be seized.
- (3) Persons who are in possession of objects referred to in paragraph 1 of this Article shall hand them over. Persons refusing to hand over the objects may be punished by a fine of up to epsilon 1.000, and in case of further rejection, they may be incarcerated. Incarceration shall last until the object is handed over or until the criminal proceedings is completed, and at the longest for two months. The procedure as regards a person in an official capacity or a responsible person in a state body, business organisation or another legal person shall be the same.
- (4) The provisions of paras. 1 and 3 of this Article shall apply to the data stored in devices for automatic or electronic data processing and media wherein such data are saved, which shall, upon the request of the court, be handed over in a legible and comprehensible form. The court and other authorities shall abide by the regulations on maintaining the confidentiality of data.
- (5) The following objects shall not be subject to seizure:
- 1) files and other documents of state bodies, publication of which would violate the obligation to keep data confidential in terms of regulations providing data confidentiality, until the competent authority decides otherwise;
- 2) letters of the accused to their defence counsel or to persons referred to in Article 109, paragraph 1, items 1, 2 and 3 of this Code save when the accused hands them over voluntarily;
- 3) recordings, extracts from the register and similar documents that are in possession of persons referred to in Article 108, item 3 of this Code and that are made by such persons in relation to the facts obtained from the accused while performing their professional service, if publication thereof would constitute violation of the obligation to keep a professional secret.
- (6) The prohibition referred to in paragraph 5, item 2 of this Article shall not apply to the defence counsel or persons exempted from the duty to testify

pursuant to Article 109, paragraph 1 of this Code if well-founded suspicion exists that they aided the accused parties in committing the criminal offence or they helped them after the criminal offence was committed or if they acted as accomplices by virtue of concealment.

- (7) The ruling referred to in paragraph 3 of this Article shall be issued by the investigative judge during the investigation and by the Chair of the Panel after an indictment has been brought.
- (8) The Panel referred to in Article 24, paragraph 7 of this Code shall decide on the appeal against the ruling referred to in paras. 2 and 3 of this Article. An appeal against the ruling on incarceration shall not suspend enforcement.
- (9) Authorized police officers may seize objects referred to in paragraph 1 of this Article when proceeding pursuant to Articles 257 and 263 of this Code or when enforcing a court ruling.
- (10) On the occasion of seizing objects it shall be specified where they were found and they shall be described, and where appropriate, their sameness shall be ensured in another way as well. A receipt shall be issued for the seized objects.
- (11) Measures referred to in paragraph 3 of this Article may not be enforced against the suspects or accused or persons relieved of duty to testify.
- (12) Provision of Article 481 of this Code shall apply on the seizure of material benefit.

Article 86 - Denial of Disclosure or Issuing of Files

- (1) State authorities may refuse to disclose or issue their files and other documents if they deem that disclosure of their contents would cause damage to the public interests, with the exception of case referred to in Article 90 of the present Code. If disclosure or handover of files and other documents was denied, the final decision shall be made by the panel referred to in Article 24, paragraph 7 of the present Code.
- (2) Enterprises or other legal entities may request that data related to their

business operations are not publicly disclosed. The panel referred to in Article 24 paragraph 7 of the present Code shall decide on the request.

Article 87 - Inventory and Sealing of Files

- (1) An inventory of provisionally seized files that may be used as evidence shall be made. If that is not possible, the files shall be put in a cover and sealed. The owner of the files may put his/her seal on the cover.
- (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/her absence.
- (3) During the examination of files, attention shall be paid that their contents are not be disclosed to unauthorized persons

Article 89 - Obtaining Information from the Competent Public Authority for Temporary Suspension of Monetary Transactions

- (1) State Prosecutors may request that the competent public authority performs control over the financial operations of certain persons and to submit them documentation and information which can be used as evidence of a criminal offence or of the proceeds of crime, as well as information about suspicious monetary transactions.
- (2) State Prosecutors may request that the competent authority or organization temporarily suspends the payment, or the issuing of suspicious money, securities and objects, at the longest for six months.
- (3) State Prosecutors shall specify in the motion referred to in paragraphs 1 and 2 of this Article in more detail the contents of measure of action they are requesting.
- (4) At the proposal of State Prosecutors, the court may issue a ruling ordering a temporary suspension of a certain monetary transaction when reasonable doubt exists that it constitutes a criminal offence or that it is intended for the commission or concealment of a criminal offence or proceeds of crime.

- (5) By way of the ruling referred to in paragraph 4 of this Article, the court shall order that funds in check or cash form be provisionally seized and deposited into a special account where they will be kept until the completion of the proceedings with final force and effect or until conditions for their return are met.
- (6) An appeal against the ruling referred to in paragraph 4 of this Article may be filed by the parties and the defense attorney, or the owner of funds or his/her proxy or the legal person from whom the funds have been provisionally seized. Such an appeal shall be decided upon by the panel referred to in Article 24, paragraph 6 of the present Code.

9. MEASURES OF SECRET SURVEILLANCE

Article 157 - Types of Secret Surveillance Measures and Conditions for Their Application

- (1) If grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of this Code and evidence cannot be obtained in another manner or their obtaining would request a disproportional risk or endangering the lives of people, measures of secret surveillance may be ordered against those persons:
- 1) secret surveillance and technical recording of telephone conversations i.e. other communication carried out through means for distance technical communication as well as private conversations held in private or public premises or in the open air;
- 2) secret photographing and video recording in private premises;
- 3) secret supervision and technical recording of persons and objects.
- (2) If grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of this Code and circumstances of the case indicate that evidence shall be collected with a minimum violation of the right to privacy,

measures of secret surveillance may be ordered against those persons:

- 1) simulated purchase of objects or persons and simulated giving and taking of bribe:
- 2) supervision over the transportation and delivery of objects of criminal offence;
- 3) recording conversations upon previous informing and obtaining the consent of one of interlocutors;
- 4) use of undercover investigators and cooperative witnesses.
- (3) Measures referred to in paragraph 1, item 1 of this Article may be also ordered against persons for whom there are grounds for suspicion that they have been conveying to the offender or from the offender of criminal offences referred to in Article 158 of this Code messages in connection to the criminal offence, or that the offender has been using their telephone lines or other electronic communication devices.
- (4) Enforcement of measures referred to in paragraph 2, items 1, 3 and 4 of this Article shall not constitute incitement to commit a criminal offence.

Article 158 - Criminal Offences for Which Measures of Secret Surveillance May Be Ordered

The measures referred to in Article 157 of this Code may be ordered for the following criminal offences:

- 1) punishable by imprisonment of ten years or a more severe sentence;
- 2) having elements of organized crime;
- 3) having elements of corruption, as follows: money laundering, causing false bankruptcy, abuse of assessment, passive bribery, active bribery, disclosure of an official secret, trading in influence, as well as abuse of authority in economy,

abuse of an official position and fraud in the conduct of an official duty punishable by imprisonment of eight years or a more serious sentence;

- 4) abduction, extortion, blackmail, meditation in prostitution, displaying pornographic material, usury, tax and contributions evasion, smuggling, unlawful processing, disposal and storing of dangerous substances, attack on a person acting in an official capacity during performance on an official duty, obstruction of the pleading process, criminal association, unlawful keeping of weapons and explosions, illegal crossing of the state border and smuggling in human beings.
- 5) against the security of computer data.

Article 159 - Competence for Ordering Measures of Secret Surveillance and Their Duration

- (1) Measures referred to in Article 157, paragraph 1 of this Code shall be ordered by a written order by the investigative judge at the motion of the Public Prosecutor containing a statement of reasons. Measures referred to in Article 157, paragraph 2 of this Code shall be ordered by a written order by the Public Prosecutor at the motion of police authorities containing a statement of reasons. The motion containing a statement of reasons shall be delivered in a closed envelope bearing the designation MSS Measures of Secret Surveillance.
- (2) The motion and the order referred to in paragraph 1 of this Article shall contain: the type of measure, data on the person against whom the measure is enforced, grounds for well-founded suspicion, the manner of measure enforcement, its goal, scope and duration. If it is a measure of engagement of an undercover agent and collaborator, the motion and the order shall also contain the use of false documents and technical devices for the transfer and recording of voice, image and video, participation in the conclusion of legal affairs, as well as the reasons justifying the engagement of a person who is not a police officer as an undercover agent and cooperative witness.
- (3) The motion and the order for ordering measures shall become an integral part of the criminal file and should contain available data on the person against

whom they are ordered, the criminal offence because of which they are ordered, the facts on basis of which the need to take them originates, duration term that needs to be suitable to achieving the objective of measure, manner, scope and place for the measures to be implemented.

- (4) As an exception, if the written order can not be issued in time and risk of delay exists, application of measure referred to in Article 157 of this Code may begin on the strength of a oral order of the investigative judge, i.e., Public Prosecutor. In that case, a written order must be obtained within 12 hours following the issue of the oral order.
- (5) Measures referred to in Article 157, paragraphs 1 and 2, items 2, 3 and 4 of this Code may last only as long as necessary, at the longest for four months, although for valid reasons they may be prolonged for three more months. The motion for taking the measure referred to in Article 157, paragraph 2, item 1 of this Code may refer only to one simulated act, and all subsequent motions for the application of this measure against the same person shall contain a statement of reasons justifying the repeated application of this measure. The application of measure shall be terminated as soon as reasons for its application cease.
- (6) In addition to the order for the application of measure referred to in Article 157, paragraph 1, item 1 of this Code, the investigative judge shall issue a separate order containing solely the telephone number or e-mail address and the duration of the measure in question, and this order shall be delivered to business organisations referred to in paragraph 7 of this Article during the course of the application of the measure by the police authorities.
- (7) Postal agencies, other business organizations and legal persons registered for transmission of information shall enable the police authorities to enforce the measure referred to in Article 157, paragraph 1 of this Code. Persons acting in an official capacity and responsible persons involved in the process of passing the order and execution of the measures referred to in Article 157 of this Code shall keep as an official secret all the data they have learned in the course of this process.
- (8) If, on the occasion of the enforcement of measures of secret surveillance, data and notifications are registered referring to some other persons for whom

grounds for suspicion exist that s/he had committed a criminal offence for which a measure of secret surveillance was ordered, or some other criminal offence, that part of the recording shall be copied and forwarded to the Public Prosecutor, and it may be used as evidence only for criminal offences referred to in Article 158 of this Code.

(9) The Public Prosecutor and the investigative judge shall, in an appropriate way (by coping records or official annotations without personal data, removal of an official annotation from the files and alike), prevent unauthorised persons, the suspects or their defence counsel to establish the identity of persons who have enforced the measures referred to in Article 157 of this Code and the undercover agents and collaborators. If such persons are to be questioned as witnesses, the Court shall act in the manner provided for in Articles 120-123 of this Code.

Article 160 - Enforcement of Measures of Secret Surveillance

- (1) The measures referred to in Article 157 of this Code shall be enforced by the police authorities in such a manner that the privacy of persons not subject to these measures be disturbed to the least extent possible.
- (2) Undercover agent and collaborator may be an authorized police officer, employee in another state body, authorized police officer of another state or, as an exception, if the measure can not be enforced in another manner, some other person.
- (3) Undercover agents and collaborator may not be persons for whom well-founded suspicion exists that they were or that they currently are members of a criminal organization or group or persons who have been convicted for criminal offences referred to in Article 22, item 8 of this Code.
- (4) Undercover agent and collaborator may participate in legal dealings by using false documents, and in collecting information they may use technical devices for the transfer and recording of sound, image and video.
- (5) Authorised police officer enforcing the measure shall keep records on each

measure taken and report periodically to the Public Prosecutor, that is, investigative judge on the enforcement of measures. If the Public Prosecutor, i.e., investigative judge ascertains that the need for enforcement of the ordered measures does not exist any more, s/he shall issue and order on their discontinuance.

- (6) Upon the enforcement of measures referred to in Article 157 of this Code the police authorities shall submit to the Public Prosecutor a final report and other material obtained by the enforcement of measures.
- (7) Should the Public Prosecutor decide not to initiate a criminal proceedings against a suspect, s/he shall forward to the investigative judge the material obtained through the application of Article 157 of this Code, in a closed cover bearing the designation MSS, and the investigative judge shall order that the material be destroyed in the presence of the Public Prosecutor and the investigative judge. The investigative judge shall compose a record thereon.
- (8) The investigative judge shall proceed in the manner described in paragraph 7 of this Article if the Public Prosecutor orders that investigation be conducted against the suspect who was subjected to measures of secret surveillance, when the results obtained or parts of the results are not indispensable for the conduct of the criminal proceedings.
- (9) In cases referred to in paras. 7 and 8 of this Article, data shall be considered as classified within the meaning of regulation prescribing data confidentiality

Article 161 - Legally Invalid Evidence

- (1) If the measures referred to in Article 157 of this Code were taken contrary to the provisions of this Code or contrary to the order of the investigative judge or the Public Prosecutor, the collected information may not serve as grounds for the judgment.
- (2) Provisions of Article 211 paragraph 1, Article 293 paragraph 5, Article 356 paragraph 4, and Article 392 paragraph 4 of this Code shall apply accordingly with regard to the recordings made contrary to the provisions of this Article and

Article 157 of this Code. Article 162 - Passing Information to Persons against Whom Measure of Secret Surveillance Was Enforced When a Criminal proceedings Is Not Initiated (1) Before the material obtained through the enforcement of measures of secret surveillance in cases referred to in Article 160, paragraphs 7 and 8 of this Code is destroyed, the investigative judge shall inform the person against whom the measure was taken, and that person shall be entitled to examine the collected material. (2) If there is a reasonable concern that passing information to the person referred to in paragraph 1 of this Article or examination of the collected material by such person could constitute a serious threat to the lives and health of people or could engender any investigation underway or if there are any other justifiable reasons, the investigative judge may, based on an opinion of the Public Prosecutor, decide that the person against whom the measure was taken not be informed and allowed to examine the collected material. **Article 15 – Conditions and safeguards** Criminal Procedure Code, Articles 76, 83 and 86 1 Each Party shall ensure that the establishment, implementation and In article 14 I put all relevant provisions application of the powers and procedures provided for in this Section are subject to conditions and safequards 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 safequards 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.

| Criminal Procedure Code, Articles 76, 83 and 86 In article 14 I put all relevant provisions |
|---|
| |
| |
| Criminal Procedure Code, Articles 76, 83 and 86 In article 14 I put all relevant provisions |
| |

| 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. | |
| Article 18 - Production order | Criminal Procedure Code, Articles 76, 83 and 86 |
| 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. | In article 14 I put all relevant provisions |
| 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. | |
| Article 19 - Search and seizure of stored computer data | Criminal Procedure Code, Articles 76, 83 and 86 |
| 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: | , , , , , , , , , , , , , , , , , , , |
| a a computer system or part of it and computer data stored | |

therein; and

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

in its territory.

- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
- a seize or similarly secure a computer system or part of it or a computer-data storage medium;
 - b make and retain a copy of those computer data;
 - c maintain the integrity of the relevant stored computer data;
 - d render inaccessible or remove those computer data in the accessed computer system.
- 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 20 - Real-time collection of traffic data

- Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
 - a collect or record through the application of technical means on the territory of that Party, and
- b compel a service provider, within its existing technical capability:

Criminal Procedure Code, Articles 237

9. MEASURES OF SECRET SURVEILLANCE

Article 157 - Types of Secret Surveillance Measures and Conditions for Their Application

(1) If grounds for suspicion exist that a person has individually or in complicity

- means on the territory of that Party; or
- collection or recording of, traffic data, in real-time, associated with specified against those persons: communications in its territory transmitted by means of a computer system.
- 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 2) secret photographing and video recording in private premises; technical means on that territory.
- Each Party shall adopt such legislative and other measures as may be 3) secret supervision and technical recording of persons and objects. 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.
- The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

to collect or record through the application of technical with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of this Code and evidence cannot be obtained in to co-operate and assist the competent authorities in the another manner or their obtaining would request a disproportional risk or endangering the lives of people, measures of secret surveillance may be ordered

- 1) secret surveillance and technical recording of telephone conversations i.e. Where a Party, due to the established principles of its domestic legal other communication carried out through means for distance technical communication as well as private conversations held in private or public premises or in the open air;

 - (2) If grounds for suspicion exist that a person has individually or in complicity with others committed, is committing or is preparing to commit criminal offences referred to in Article 158 of this Code and circumstances of the case indicate that evidence shall be collected with a minimum violation of the right to privacy, measures of secret surveillance may be ordered against those persons:
 - 1) simulated purchase of objects or persons and simulated giving and taking of bribe:
 - 2) supervision over the transportation and delivery of objects of criminal offence:
 - 3) recording conversations upon previous informing and obtaining the consent of one of interlocutors:
 - 4) use of undercover investigators and cooperative witnesses.
 - (3) Measures referred to in paragraph 1, item 1 of this Article may be also ordered against persons for whom there are grounds for suspicion that they have been conveying to the offender or from the offender of criminal offences referred to in Article 158 of this Code messages in connection to the criminal offence, or that the offender has been using their telephone lines or other

electronic communication devices.

(4) Enforcement of measures referred to in paragraph 2, items 1, 3 and 4 of this Article shall not constitute incitement to commit a criminal offence.

Article 158 - Criminal Offences for Which Measures of Secret Surveillance May Be Ordered

The measures referred to in Article 157 of this Code may be ordered for the following criminal offences:

- 1) punishable by imprisonment of ten years or a more severe sentence;
- 2) having elements of organized crime;
- 3) having elements of corruption, as follows: money laundering, causing false bankruptcy, abuse of assessment, passive bribery, active bribery, disclosure of an official secret, trading in influence, as well as abuse of authority in economy, abuse of an official position and fraud in the conduct of an official duty punishable by imprisonment of eight years or a more serious sentence;
- 4) abduction, extortion, blackmail, meditation in prostitution, displaying pornographic material, usury, tax and contributions evasion, smuggling, unlawful processing, disposal and storing of dangerous substances, attack on a person acting in an official capacity during performance on an official duty, obstruction of the pleading process, criminal association, unlawful keeping of weapons and explosions, illegal crossing of the state border and smuggling in human beings.
- 5) against the security of computer data.

Article 159 - Competence for Ordering Measures of Secret Surveillance and Their Duration

(1) Measures referred to in Article 157, paragraph 1 of this Code shall be ordered by a written order by the investigative judge at the motion of the Public

Prosecutor containing a statement of reasons. Measures referred to in Article 157, paragraph 2 of this Code shall be ordered by a written order by the Public Prosecutor at the motion of police authorities containing a statement of reasons. The motion containing a statement of reasons shall be delivered in a closed envelope bearing the designation MSS - Measures of Secret Surveillance.

- (2) The motion and the order referred to in paragraph 1 of this Article shall contain: the type of measure, data on the person against whom the measure is enforced, grounds for well-founded suspicion, the manner of measure enforcement, its goal, scope and duration. If it is a measure of engagement of an undercover agent and collaborator, the motion and the order shall also contain the use of false documents and technical devices for the transfer and recording of voice, image and video, participation in the conclusion of legal affairs, as well as the reasons justifying the engagement of a person who is not a police officer as an undercover agent and cooperative witness.
- (3) The motion and the order for ordering measures shall become an integral part of the criminal file and should contain available data on the person against whom they are ordered, the criminal offence because of which they are ordered, the facts on basis of which the need to take them originates, duration term that needs to be suitable to achieving the objective of measure, manner, scope and place for the measures to be implemented.
- (4) As an exception, if the written order can not be issued in time and risk of delay exists, application of measure referred to in Article 157 of this Code may begin on the strength of a oral order of the investigative judge, i.e., Public Prosecutor. In that case, a written order must be obtained within 12 hours following the issue of the oral order.
- (5) Measures referred to in Article 157, paragraphs 1 and 2, items 2, 3 and 4 of this Code may last only as long as necessary, at the longest for four months, although for valid reasons they may be prolonged for three more months. The motion for taking the measure referred to in Article 157, paragraph 2, item 1 of this Code may refer only to one simulated act, and all subsequent motions for the application of this measure against the same person shall contain a statement of reasons justifying the repeated application of this measure. The application of measure shall be terminated as soon as reasons for its application

cease.

- (6) In addition to the order for the application of measure referred to in Article 157, paragraph 1, item 1 of this Code, the investigative judge shall issue a separate order containing solely the telephone number or e-mail address and the duration of the measure in question, and this order shall be delivered to business organisations referred to in paragraph 7 of this Article during the course of the application of the measure by the police authorities.
- (7) Postal agencies, other business organizations and legal persons registered for transmission of information shall enable the police authorities to enforce the measure referred to in Article 157, paragraph 1 of this Code. Persons acting in an official capacity and responsible persons involved in the process of passing the order and execution of the measures referred to in Article 157 of this Code shall keep as an official secret all the data they have learned in the course of this process.
- (8) If, on the occasion of the enforcement of measures of secret surveillance, data and notifications are registered referring to some other persons for whom grounds for suspicion exist that s/he had committed a criminal offence for which a measure of secret surveillance was ordered, or some other criminal offence, that part of the recording shall be copied and forwarded to the Public Prosecutor, and it may be used as evidence only for criminal offences referred to in Article 158 of this Code.
- (9) The Public Prosecutor and the investigative judge shall, in an appropriate way (by coping records or official annotations without personal data, removal of an official annotation from the files and alike), prevent unauthorised persons, the suspects or their defence counsel to establish the identity of persons who have enforced the measures referred to in Article 157 of this Code and the undercover agents and collaborators. If such persons are to be questioned as witnesses, the Court shall act in the manner provided for in Articles 120-123 of this Code.

Article 160 - Enforcement of Measures of Secret Surveillance

- (1) The measures referred to in Article 157 of this Code shall be enforced by the police authorities in such a manner that the privacy of persons not subject to these measures be disturbed to the least extent possible.
- (2) Undercover agent and collaborator may be an authorized police officer, employee in another state body, authorized police officer of another state or, as an exception, if the measure can not be enforced in another manner, some other person.
- (3) Undercover agents and collaborator may not be persons for whom well-founded suspicion exists that they were or that they currently are members of a criminal organization or group or persons who have been convicted for criminal offences referred to in Article 22, item 8 of this Code.
- (4) Undercover agent and collaborator may participate in legal dealings by using false documents, and in collecting information they may use technical devices for the transfer and recording of sound, image and video.
- (5) Authorised police officer enforcing the measure shall keep records on each measure taken and report periodically to the Public Prosecutor, that is, investigative judge on the enforcement of measures. If the Public Prosecutor, i.e., investigative judge ascertains that the need for enforcement of the ordered measures does not exist any more, s/he shall issue and order on their discontinuance.
- (6) Upon the enforcement of measures referred to in Article 157 of this Code the police authorities shall submit to the Public Prosecutor a final report and other material obtained by the enforcement of measures.
- (7) Should the Public Prosecutor decide not to initiate a criminal proceedings against a suspect, s/he shall forward to the investigative judge the material obtained through the application of Article 157 of this Code, in a closed cover bearing the designation MSS, and the investigative judge shall order that the material be destroyed in the presence of the Public Prosecutor and the investigative judge. The investigative judge shall compose a record thereon.

- (8) The investigative judge shall proceed in the manner described in paragraph 7 of this Article if the Public Prosecutor orders that investigation be conducted against the suspect who was subjected to measures of secret surveillance, when the results obtained or parts of the results are not indispensable for the conduct of the criminal proceedings.
- (9) In cases referred to in paras. 7 and 8 of this Article, data shall be considered as classified within the meaning of regulation prescribing data confidentiality

Article 161 - Legally Invalid Evidence

- (1) If the measures referred to in Article 157 of this Code were taken contrary to the provisions of this Code or contrary to the order of the investigative judge or the Public Prosecutor, the collected information may not serve as grounds for the judgment.
- (2) Provisions of Article 211 paragraph 1, Article 293 paragraph 5, Article 356 paragraph 4, and Article 392 paragraph 4 of this Code shall apply accordingly with regard to the recordings made contrary to the provisions of this Article and Article 157 of this Code.

Article 162 - Passing Information to Persons against Whom Measure of Secret Surveillance Was Enforced When a Criminal proceedings Is Not Initiated

- (1) Before the material obtained through the enforcement of measures of secret surveillance in cases referred to in Article 160, paragraphs 7 and 8 of this Code is destroyed, the investigative judge shall inform the person against whom the measure was taken, and that person shall be entitled to examine the collected material.
- (2) If there is a reasonable concern that passing information to the person referred to in paragraph 1 of this Article or examination of the collected material by such person could constitute a serious threat to the lives and health of people or could engender any investigation underway or if there are any other justifiable reasons, the investigative judge may, based on an opinion of the

| | Public Prosecutor, decide that the person against whom the measure was taken not be informed and allowed to examine the collected material. |
|---|---|
| Article 21 – Interception of content data | Criminal Procedure Code, Articles 237 |
| 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: ito collect or record through the application of technical means on the territory of that Party, or iito co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | SEE ARTICLE 20 |
| Section 3 – Jurisdiction | |
| Article 22 – Jurisdiction | Section 2 of the Criminal Procedure Code, Articles 23-30 |
| 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 | The courts shall adjudicate all cases within the limits of their subject matter jurisdiction prescribed by the law. |

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

- on board an aircraft registered under the laws of that Party; or
- 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.
- specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
- 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 basis of his or her nationality, after a request for extradition.
- This Convention does not exclude any criminal jurisdiction exercised lay judges. 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.

Article 24

Unless otherwise determined by this Code, first instance courts sit in panels of two judges and three lay judges when considering criminal offences punishable by imprisonment for a term of fifteen years or more severe punishment, and in Each Party may reserve the right not to apply or to apply only in panels of one judge and two lay judges when considering criminal offences punishable by a lenient punishment. A single judge shall sit in the first instance court when the provisions on summary proceedings are applicable.

Unless otherwise determined by this Code, Second instance courts sit in panels of five judges when considering criminal offences punishable by imprisonment for a term of fifteen years or more severe punishment and in panels of three territory and it does not extradite him or her to another Party, solely on the judges when considering criminal offences punishable by a lenient punishment. At a trial at second instance the court shall sit in a panel of two judges and three

Third instance courts sit in panels of five judges.

The investigating judge of the first instance court shall perform investigatory actions.

The president of the court and the president of the panel shall decide on cases as provided in this Code.

First instance courts, sitting in a panel of three judges shall decide on appeals against rulings of the investigating judge and other rulings when prescribed by this Code, render decisions in the first instance outside the trial, conduct the proceedings and render a judgement on the request seeking execution of a criminal judgment of a foreign court, and make proposals in cases determined by this Code or other Law.

When it decides on a request for extraordinary mitigation of punishment, the court sits in a panel of five judges when considering criminal offences for which the Criminal Code sets forth a punishment by imprisonment for a term of fifteen vears or more severe punishment, and in a panel of three judges when considering criminal offences punishable by a lenient punishment and when it decides on a request for the review of legality of a final judgement.

When deciding on a motion for protection of legality the court shall sit in a panel of five judges.

Unless otherwise determined by this Code, higher courts also sit in a panel of three judges when they decide on cases not specified in the preceding paragraphs of this Article.

Article 25 - General Rules of Determining Territorial Jurisdiction

- (1) As a rule, the court having territorial jurisdiction shall be the one within whose territory criminal offence was committed or attempted.
- (2) A personal action at law may be lodged with the court within the territory of which the accused has permanent or temporary residence.
- (3) If the criminal offence was committed or attempted within the territory of several courts or on the border of those territories, or if it is uncertain within which territory the offence has been committed or attempted, the court of appropriate jurisdiction shall be the one which has first instituted the procedure upon the indictment of the authorized prosecutor, whereas in preliminary investigation and investigation the court of appropriate jurisdiction shall be the one that was the first to take an action upon the prosecutor's motion.

Article 26 - Territorial Jurisdiction of Courts in Cases of Offences Committed on a National Ship or Aircraft

If a criminal offence was committed on a national ship or aircraft while it was in a home port or airport, the court of appropriate jurisdiction shall be the one whose territory includes that port or airport. In other cases where a criminal offence has been committed on a national ship or aircraft, the court of appropriate jurisdiction shall be the court whose territory includes the home port of the ship or home airport of the aircraft or national port or airport where the vessel or aircraft stops for the first time.

Article 27 - Territorial Jurisdiction for an Offence Committed by Means of Media

(1) If a criminal offence was committed by means of press, the court of appropriate jurisdiction shall be the one within whose territory the paper was printed. If this location is unknown or if the paper was printed abroad, the court of appropriate jurisdiction shall be the one within whose territory the printed

paper is distributed.

- (2) If according to law the author of the text is responsible, the court of appropriate jurisdiction shall be the one within whose territory the author has permanent residence or the court within whose territory the event to which the text refers took place.
- (3) Provisions of paras. 1 and 2 of this Article shall also be applied accordingly to cases where the statement or text was released via a radio, television station or other mass media.

Article 28 - Territorial Jurisdiction in Case When the Place of Commission of a Criminal Offence is Unknown

- (1) If the place of the commission of a criminal offence is unknown or if that place is outside of Montenegro, the court of appropriate jurisdiction shall be the one within whose territory the accused has temporary or permanent residence.
- (2) If the procedure is already pending before the court of the accused's temporary or permanent residence, when the place of the commission has been determined, this court shall retain its jurisdiction.
- (3) If neither the place of the commission of the criminal offence nor the temporary or permanent residence of the accused is known, or if both are outside the territory of Montenegro, the court of appropriate jurisdiction shall be the one within whose territory the accused is placed under arrest or turned himself/herself in.

Article 29 - Territorial Jurisdiction in Cases of Criminal Offences Committed in Montenegro and Abroad

If a person has committed a criminal offence both in Montenegro and abroad, the court of appropriate jurisdiction shall be the one that has jurisdiction over the criminal offence committed in Montenegro.

Article 30 - Designated Territorial Jurisdiction (Forum ordinatum)

If it is not possible to ascertain which court has territorial jurisdiction under the provisions of this Code, the Supreme Court of Montenegro (hereinafter referred to as the: the Supreme Court) shall designate one of the courts of subjectmatter jurisdiction to conduct the proceedings.

Chapter III - International co-operation

Article 24 - Extradition

- 1 a This article applies to extradition between Parties for the criminal Matters offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties | The assumptions for the extradition shall be as follows: concerned by deprivation of liberty for a maximum period of at least one the person whose extradition is requested is not a national of the Republic of year, or by a more severe penalty.
- Where a different minimum penalty is to be applied under an territory of Montenegro, against Montenegro or its national; arrangement agreed on the basis of uniform or reciprocal legislation or an 24), applicable between two or more parties, the minimum penalty provided committed; for under such arrangement or treaty shall apply.
- deemed to be included as extraditable offences in any extradition treaty detained or examined as an accused; existing between or among the Parties. The Parties undertake to include such the foreigner whose extradition is requested has not been already convicted by between or among them.
- of this article.
- 4 Parties that do not make extradition conditional on the existence of a treaty national of Montenegro; shall recognise the criminal offences referred to in paragraph 1 of this article the identity of the person claimed has been established; as extraditable offences between themselves.
- requested Party or by applicable extradition treaties, including the grounds on it does not concern a minor offence (Article 9 of the Criminal Code). which the requested Party may refuse extradition.
- 6 If extradition for a criminal offence referred to in paragraph 1 of this article

Article 11 of the Law on International Legal Assistance in Criminal

Montenegro (hereinafter referred to as Montenegro);

the offence for which extradition is requested has not been committed in the

the offence motivating the request for extradition is a criminal offence both extradition treaty, including the European Convention on Extradition (ETS No. under the domestic law and under the law of the country in which it has been

the criminal prosecution or enforcement of criminal sanction has not been 2 The criminal offences described in paragraph 1 of this article shall be barred by the lapse of time under domestic law before the foreigner has been

offences as extraditable offences in any extradition treaty to be concluded a domestic court for the same offence; or he has not been acquitted of the same offence by the domestic court in a final and legally binding manner, 3 If a Party that makes extradition conditional on the existence of a treaty except if the requirements prescribed under the Criminal Procedure Code for receives a request for extradition from another Party with which it does not the retrial have been met; or criminal proceedings have not been instituted in have an extradition treaty, it may consider this Convention as the legal basis Montenegro for the same offence against Montenegro; or the security for the for extradition with respect to any criminal offence referred to in paragraph 1 fulfilment of property law claim of the victim has been provided if the proceedings have been instituted for the offence committed against the

there is sufficient evidence for a grounded suspicion that the foreigner claimed 5 Extradition shall be subject to the conditions provided for by the law of the committed the criminal offence or a final judgement has been passed,

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 LAW ON INTERNATIONAL LEGAL ASSISTANCE IN CRIMINAL MATTERS offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
- necessary to carry out the obligations set forth in Articles 27 through 35.
- communication, including fax or e-mail, to the extent that such means persons and temporary seizure of items. provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where Article 4 required by the requested Party. The requested Party shall accept and The Ministry responsible for the judiciary (hereinafter referred to as the respond to the request by any such expedited means of communication.
- 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance to foreign judicial authorities and vice versa. assistance shall be subject to the conditions provided for by the law of the In cases when this has been provided for under an international agreement or

Articles 3, 4, 5 and 6 of the Law on International Legal Assistance in **Criminal Matters**

Article 3

International legal assistance shall include extradition of the accused and 2 Each Party shall also adopt such legislative and other measures as may be sentenced persons, transfer and assuming of criminal prosecution, enforcement of foreign criminal verdicts, delivery of documents, writs and other cases associated with the criminal proceedings in the requesting state, as well as the 3 Each Party may, in urgent circumstances, make requests for mutual undertaking of certain procedural actions such as: hearing of the accused, assistance or communications related thereto by expedited means of witnesses and experts, crime scene investigation, search of premises and

Ministry) shall be a central communication authority through which domestic judicial authorities shall forward letters rogatory for international legal

grounds on which the requested Party may refuse co-operation. The relation to the offences referred to in Articles 2 through 11 solely on the letters rogatory for international legal assistance through diplomatic channels. ground that the request concerns an offence which it considers a fiscal Without prejudice to the above, if provided for under an international offence.

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 international legal assistance in accordance with the law. offence under its laws.

requested Party or by applicable mutual assistance treaties, including the where there is reciprocity, the Ministry shall submit letters rogatory to the central communication authority of the requested state, and in cases where requested Party shall not exercise the right to refuse mutual assistance in there is no such agreement or reciprocity, the Ministry shall deliver and receive

agreement, domestic judicial authorities may deliver letters rogatory for international legal assistance to a foreign judicial authority directly and they 5 Where, in accordance with the provisions of this chapter, the requested shall be obliged to deliver the copy of the letter rogatory to the Ministry.

Party is permitted to make mutual assistance conditional upon the existence In urgent cases, provided that there is reciprocity, letter rogatory for of dual criminality, that condition shall be deemed fulfilled, irrespective of international legal assistance may be delivered through the National Central Bureau - INTERPOL.

The higher court and the state prosecutor shall be responsible for provision of

Article 5

The Ministry shall deliver, without delay, the letters rogatory from foreign judicial authorities to domestic judicial authorities, except in cases when it is obvious that the letter rogatory should be rejected.

The permissibility and the method of enforcement of the action which is the subject matter of a foreign judicial authority shall be decided by the court in accordance with domestic legislation and ratified international agreements.

Article 6

The basis for provision of international criminal assistance shall be that the offence for which the provision of international legal assistance is requested is a criminal offence both under the domestic law and under the law of the requesting country the judicial authority of which presented the letter rogatory.

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.

Law on International Legal Assistance in Criminal Matters in the absence of applicable international agreements

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.

Article 27 - Procedures pertaining to mutual assistance requests in Article 4 of the Law on International Legal Assistance in Criminal 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 Article 4 requested Parties, the provisions of paragraphs 2 through 9 of this article The Ministry responsible for the judiciary (hereinafter referred to as the shall apply. The provisions of this article shall not apply where such treaty any or all of the remainder of this article in lieu thereof.
- for sending and answering requests for mutual assistance, the execution of execution.
- The central authorities shall communicate directly with each other;
- Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the authorities designated in pursuance of this paragraph;
- shall ensure that the details held on the register are correct at all times.
- Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except international legal assistance in accordance with the law. where incompatible with the law of the requested Party.
- The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
- the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
- it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.
- The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its

Matters

Ministry) shall be a central communication authority through which domestic arrangement or legislation exists, unless the Parties concerned agree to apply judicial authorities shall forward letters rogatory for international legal assistance to foreign judicial authorities and vice versa.

2 a Each Party shall designate a central authority or authorities responsible In cases when this has been provided for under an international agreement or where there is reciprocity, the Ministry shall submit letters rogatory to the such requests or their transmission to the authorities competent for their central communication authority of the requested state, and in cases where there is no such agreement or reciprocity, the Ministry shall deliver and receive letters rogatory for international legal assistance through diplomatic channels.

Without prejudice to the above, if provided for under an international agreement, domestic judicial authorities may deliver letters rogatory for the Secretary General of the Council of Europe the names and addresses of international legal assistance to a foreign judicial authority directly and they shall be obliged to deliver the copy of the letter rogatory to the Ministry.

The Secretary General of the Council of Europe shall set up and keep In urgent cases, provided that there is reciprocity, letter rogatory for updated a register of central authorities designated by the Parties. Each Party international legal assistance may be delivered through the National Central Bureau - INTERPOL.

The higher court and the state prosecutor shall be responsible for provision of

authorities.

- 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
- 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
- 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
- 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.
- b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).
- c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.
- d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.
- e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 - Confidentiality and limitation on use

- 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
- 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:
- a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
- b not used for investigations or proceedings other than those stated in the request.
- 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
- 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Article 29 - Expedited preservation of stored computer data

- 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

Law on International Legal Assistance in Criminal Matters in the absence of applicable international agreements

Law on International Legal Assistance in Criminal Matters in the absence of applicable international agreements

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.
- 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

Law on International Legal Assistance in Criminal Matters in the absence of applicable international agreements

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. Disclosure of traffic data under paragraph 1 may only be withheld if: the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests. Article 31 - Mutual assistance regarding accessing of stored computer International legal assistance in the cases related to cyber crime is data currently realized through the National Office of Interpol in Podgorica. 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation. Article 32 - Trans-border access to stored computer data with International legal assistance in the cases related to cyber crime is consent or where publicly available currently realized through the National Office of Interpol in Podgorica. A Party may, without the authorisation of another Party: access publicly available (open source) stored computer data, regardless of where the data is located geographically; or access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. Article 33 - Mutual assistance in the real-time collection of traffic International legal assistance in the cases related to cyber crime is currently realized through the National Office of Interpol in Podgorica. data 1 The Parties shall provide mutual assistance to each other in the real-time

collection of traffic data associated with specified communications in their

territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

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

Article 34 - Mutual assistance regarding the interception of content International legal assistance in the cases related to cyber crime is 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.

currently realized through the National Office of Interpol in Podgorica.

Article 35 - 24/7 Network

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

- the provision of technical advice;
- the preservation of data pursuant to Articles 29 and 30;
- the collection of evidence, the provision of legal information, and locating of suspects.
- 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.
- 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.

International legal assistance in the cases related to cyber crime is currently realized through the National Office of Interpol in Podgorica.

Article 42 - Reservations

By a written notification addressed to the Secretary General of the Council of March 2010 - Or. Engl. Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it In accordance with Article 9, paragraph 4, and with regard to Article 9, avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article paragraph 1, item e, of the Convention, Montenegro declares that obtaining 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. | storage of computer data shall not be considered offences in case the person

Reservation contained in the instrument of ratification deposited on 3

child pornography through computer systems for oneself and other persons and possession of child pornography in computer systems or on mediums for displayed in these materials turned fourteen years of age and gave his/her consent.

Period covered: 1/7/2010 -

The preceding statement concerns Article(s): 9

Reservation contained in the instrument of ratification deposited on 3 March 2010 - Or. Engl.

In accordance with Article 9, paragraph 4, and with regard to Article 9, paragraph 2, item b, of the Convention, Montenegro declares that materials which visually display face by which it can be concluded that the person is a minor engaged in an explicit act as stated in Article 9, paragraph 2, item b, of this Convention shall not be considered child pornography.

Period covered: 1/7/2010 -

The preceding statement concerns Article(s): 9

Reservation contained in the instrument of ratification deposited on 3 March 2010 - Or. Engl.

In accordance with Article 14, paragraph 3, and with regard to Article 20, of the Convention, Montenegro declares that measures from Article 20 of the Convention shall be applied solely on the basis of the decision of a competent Montenegrin court, if it is necessary for conducting a criminal procedure or for reasons of safety in Montenegro.

Period covered: 1/7/2010 -

The preceding statement concerns Article(s): 14, 20

Declaration contained in the instrument of ratification deposited on 3 March 2010 - Or. Engl.

In accordance with Article 24, paragraph 7, of the Convention, Montenegro declares that the authority responsible for making and receiving requests for extradition in the absence of an agreement is the Ministry of Justice of Montenegro, address: Vuka Karadzica 3, 81 000 Podgorica, while the authority responsible for making and receiving requests for provisional arrest in the absence of an agreement is the NCB Interpol in Podgorica, address: Bulevar Svetog Petra Cetinjskog 22, 81 000 Podgorica.

Period covered: 1/7/2010 -

The preceding statement concerns Article(s): 24

Declaration contained in the instrument of ratification deposited on 3 March 2010 - Or. Engl.

In accordance with Article 27, paragraph 2, of the Convention, Montenegro declares that the central authority designated for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution in the absence of an agreement is the Ministry of Justice of Montenegro, address: Vuka Karadzica 3, 81 000 Podgorica.

Period covered: 1/7/2010 -

The preceding statement concerns Article(s): 27