

### Table of contents

Version 01 May 2020

[reference to the provisions of the Budapest Convention]

#### Chapter I – Use of terms

Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”

#### Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Article 2 – Illegal access

Article 3 – Illegal interception

Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

Article 7 – Computer-related forgery

Article 8 – Computer-related fraud

Article 9 – Offences related to child pornography

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

Article 11 – Attempt and aiding or abetting

Article 12 – Corporate liability

Article 13 – Sanctions and measures

Section 2 – Procedural law

Article 14 – Scope of procedural provisions

Article 15 – Conditions and safeguards

Article 16 – Expedited preservation of stored computer data

Article 17 – Expedited preservation and partial disclosure of traffic data

Article 18 – Production order

Article 19 – Search and seizure of stored computer data

Article 20 – Real-time collection of traffic data

Article 21 – Interception of content data

Section 3 – Jurisdiction

Article 22 – Jurisdiction

#### Chapter III – International co-operation

Article 24 – Extradition

Article 25 – General principles relating to mutual assistance

Article 26 – Spontaneous information

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

Article 28 – Confidentiality and limitation on use

Article 29 – Expedited preservation of stored computer data

Article 30 – Expedited disclosure of preserved traffic data

Article 31 – Mutual assistance regarding accessing of stored computer data

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

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

Article 34 – Mutual assistance regarding the interception of content data

Article 35 – 24/7 Network

*This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.*

<b>State:</b>	
<b>Signature of the Budapest Convention:</b>	N/A
<b>Ratification/accession:</b>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<b>Chapter I – Use of terms</b>	
<p><b>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”:</b></p> <p>For the purposes of this Convention:</p> <p>a “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;</p> <p>b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service</p>	<p><b>Law of Ukraine On Telecommunications No.1280-IV, 18 November 2003</b></p> <p><b>Article 1. Terms and Definitions</b></p> <p>The following terms as used herein shall have the following definitions:</p> <p>communication channel - totality of technical means designed for transmission of electric signals between two points of a telecommunication network and characterized by frequency band and transmission rate;</p> <p>data - information expressed in a format suitable for its automated processing by computation means;</p> <p>telecommunication operator - a business entity entitled to operate in the telecommunication sector and having the right to telecommunication networks maintenance and operation;</p> <p>telecommunication provider - a business entity entitled to operate in the telecommunication sector and having the right to telecommunication networks maintenance and operation and to electric communication channels transfer into use;</p> <p><i>traffic – [definition not updated]</i></p>
<b>Chapter II – Measures to be taken at the national level</b>	
<b>Section 1 – Substantive criminal law</b>	
<b>Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems</b>	
<b>Article 2 – Illegal access</b>	<b>Criminal Code of Ukraine</b>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b>Article 361. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks</b></p> <p>1. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks, which resulted in the leak, loss, counterfeiting, blocking of information, troubling the processing of information or violating the established procedure for its routing, - shall be punishable by a fine in the amount of six hundred to one thousand non-taxable minimum incomes of citizens, or by restriction of freedom for a term of two to five years, or by imprisonment for a term up to three years, with or without deprivation of right to hold certain positions or engage in certain activities for a term up to two years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.</p> <p>2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a substantial damage, - shall be punishable by imprisonment for a term of three to six years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.</p> <p><b>Note.</b> Under Articles 361 – 363-1, it is understood that physical damage is considered to be substantial if its value one hundred times and more exceeds non-taxable minimum incomes of citizens.</p>
<p><b>Article 3 – Illegal interception</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b>Criminal Code of Ukraine</b></p> <p><b>Article 163. Violation of privacy of mail, telephone conversations, telegraph and other correspondence conveyed by means of communication or via computers</b></p> <p>1. Violation of privacy of mail, telephone conversations, telegraph and other correspondence conveyed by means of communication or via computers, - shall be punishable by a fine of 50 to 100 tax-free minimum incomes, or correctional labor for a term up to two years, or restraint of liberty for a term up to three years.</p> <p>2. The same actions committed in respect of statesmen or public figures, by an official, or by use of special devices for secret reading of information, - shall be punishable by imprisonment for a term of three to seven years.</p>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION****Article 361. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks**

1. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks, which resulted in the leak, loss, counterfeiting, blocking of information, troubling the processing of information or violating the established procedure for its routing, - shall be punishable by a fine in the amount of six hundred to one thousand non-taxable minimum incomes of citizens, or by restriction of freedom for a term of two to five years, or by imprisonment for a term up to three years, with or without deprivation of right to hold certain positions or engage in certain activities for a term up to two years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.

2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a substantial damage, - shall be punishable by imprisonment for a term of three to six years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.

**Note.** Under Articles 361 – 363-1, it is understood that physical damage is considered to be substantial if its value one hundred times and more exceeds non-taxable minimum incomes of citizens.

**Article 361-2. Unauthorized sale or distribution of information with limited access which is stored in electronic computers, computer-based systems, computer networks or on mediums carrying such information**

1. Unauthorized sale or distribution of information with limited access which is stored in electronic computers, computer-based systems, computer networks or on mediums carrying such information which is created and protected in accordance with applicable legislation, - shall be punishable by a fine in the amount of five hundred to one thousand non-taxable minimum incomes of citizens, or by imprisonment for a term up to two years, with

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

confiscation of software and hardware which were used for unauthorized sale or distribution of information with limited access and which belong to the offender.

2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a large damage, - shall be punishable by imprisonment for a term of two to five years, with confiscation of software and hardware which were used for unauthorized sale or distribution of information with limited access and which belong to the offender.

**Article 362. Unauthorized actions with information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, such actions being committed by a person having the right of access thereto**

1. Unauthorized alteration, deletion, or blocking of information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, such actions being committed by a person having the right of access thereto, - shall be punishable by a fine in the amount of six hundred to one thousand non-taxable minimum incomes of citizens, or by correctional works for a term up to two years, with confiscation of software and hardware which were used for unauthorized alteration, deletion, or blocking of information and which belong to the offender.

2. Unauthorized interception or copying of information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, if such actions resulted in the leak of the information and were committed by a person having the right of access thereto, - shall be punishable by imprisonment for a term up to three years, with deprivation of right to hold certain positions or engage in certain activities for the same term and with confiscation of software and hardware which were used for interception or copying of information and which belong to the offender.

3. Actions as referred to in paragraph 1 or 2 of the present Article if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a large damage, - shall be punishable by imprisonment for a term of three to six

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for unauthorized actions with information and which belong to the offender.
<p><b>Article 4 – Data interference</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p><b>Criminal Code of Ukraine</b></p> <p><b>Article 361. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks</b></p> <p>1. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks, which resulted in the leak, loss, counterfeiting, blocking of information, troubling the processing of information or violating the established procedure for its routing, - shall be punishable by a fine in the amount of six hundred to one thousand non-taxable minimum incomes of citizens, or by restriction of freedom for a term of two to five years, or by imprisonment for a term up to three years, with or without deprivation of right to hold certain positions or engage in certain activities for a term up to two years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.</p> <p>2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a substantial damage, - shall be punishable by imprisonment for a term of three to six years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.</p> <p><b>Note.</b> Under Articles 361 – 363-1, it is understood that physical damage is considered to be substantial if its value one hundred times and more exceeds non-taxable minimum incomes of citizens.</p> <p><b>Article 361-2. Unauthorized sale or distribution of information with limited access which is stored in electronic computers, computer-based systems, computer networks or on mediums carrying such information</b></p>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

1. Unauthorized sale or distribution of information with limited access which is stored in electronic computers, computer-based systems, computer networks or on mediums carrying such information which is created and protected in accordance with applicable legislation, - shall be punishable by a fine in the amount of five hundred to one thousand non-taxable minimum incomes of citizens, or by imprisonment for a term up to two years, with confiscation of software and hardware which were used for unauthorized sale or distribution of information with limited access and which belong to the offender.

2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a large damage, - shall be punishable by imprisonment for a term of two to five years, with confiscation of software and hardware which were used for unauthorized sale or distribution of information with limited access and which belong to the offender.

**Article 362. Unauthorized actions with information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, such actions being committed by a person having the right of access thereto**

1. Unauthorized alteration, deletion, or blocking of information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, such actions being committed by a person having the right of access thereto, - shall be punishable by a fine in the amount of six hundred to one thousand non-taxable minimum incomes of citizens, or by correctional works for a term up to two years, with confiscation of software and hardware which were used for unauthorized alteration, deletion, or blocking of information and which belong to the offender.

2. Unauthorized interception or copying of information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, if such actions resulted in the leak of the information and were committed by a person having the right of access thereto, - shall be punishable by imprisonment for a term up to three years, with deprivation of right to hold certain positions or engage in

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>certain activities for the same term and with confiscation of software and hardware which were used for interception or copying of information and which belong to the offender.</p> <p>3. Actions as referred to in paragraph 1 or 2 of the present Article if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a large damage, - shall be punishable by imprisonment for a term of three to six years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for unauthorized actions with information and which belong to the offender.</p>
<p><b>Article 5 – System interference</b> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</p>	<p><b>Criminal Code of Ukraine</b></p> <p><b>Article 361. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks</b></p> <p>1. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks, which resulted in the leak, loss, counterfeiting, blocking of information, troubling the processing of information or violating the established procedure for its routing, - shall be punishable by a fine in the amount of six hundred to one thousand non-taxable minimum incomes of citizens, or by restriction of freedom for a term of two to five years, or by imprisonment for a term up to three years, with or without deprivation of right to hold certain positions or engage in certain activities for a term up to two years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.</p> <p>2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a substantial damage, - shall be punishable by imprisonment for a term of three to six years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.</p> <p><b>Note.</b> Under Articles 361 – 363-1, it is understood that physical damage is considered to be substantial if its value one hundred times and more exceeds non-taxable minimum incomes of citizens.</p>



**BUDAPEST CONVENTION****DOMESTIC LEGISLATION****Article 362. Unauthorized actions with information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, such actions being committed by a person having the right of access thereto**

1. Unauthorized alteration, deletion, or blocking of information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, such actions being committed by a person having the right of access thereto, - shall be punishable by a fine in the amount of six hundred to one thousand non-taxable minimum incomes of citizens, or by correctional works for a term up to two years, with confiscation of software and hardware which were used for unauthorized alteration, deletion, or blocking of information and which belong to the offender.
2. Unauthorized interception or copying of information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, if such actions resulted in the leak of the information and were committed by a person having the right of access thereto, - shall be punishable by imprisonment for a term up to three years, with deprivation of right to hold certain positions or engage in certain activities for the same term and with confiscation of software and hardware which were used for interception or copying of information and which belong to the offender.
3. Actions as referred to in paragraph 1 or 2 of the present Article if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a large damage, - shall be punishable by imprisonment for a term of three to six years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for unauthorized actions with information and which belong to the offender.

**Article 363-1. Obstructing operation of electronic computers, computer-based systems, computer or telecommunication networks through mass distribution of telecommunication messages**

1. Willful mass distribution of telecommunication messages without prior consent of addressees, which resulted in discontinuance or break of operation

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>of electronic computers, computer-based systems, computer or telecommunication networks, - shall be punishable by a fine in the amount of five hundred to one thousand non-taxable minimum incomes of citizens, or by restriction of freedom for a term up to three years.</p> <p>2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a substantial damage, - shall be punishable by restriction of freedom for a term up to five years, or by imprisonment for the same term, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for mass distribution of telecommunication messages and which belong to the offender.</p>
<p><b>Article 6 – Misuse of devices</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;</p> <p>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p>	<p><b>Criminal Code of Ukraine</b></p> <p><b>Article 361-1. Creating detrimental software or hardware for the purpose of their application, distribution, or sale, as well as distribution or sale of the same</b></p> <p>1. Creating detrimental software or hardware for the purpose of their application, distribution, or sale, as well as distribution or sale of the same, which are designed for unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks, - shall be punishable by a fine in the amount of five hundred to one thousand non-taxable minimum incomes of citizens, or by correctional works for a term up to two years, or by imprisonment for the same term, with confiscation of software and hardware which are designed for unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks and which belong to the offender.</p> <p>2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a large damage, - shall be punishable by imprisonment for a term up to five years, with confiscation of software and hardware which are designed for unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks and which belong to the offender.</p> <p><b>Reservation contained in the instrument of ratification deposited on 10 March 2006</b></p> <p>Ukraine reserves the right not to apply paragraph 1 of Article 6 of the Convention concerning the establishment of criminal liability for the production, procurement for use and otherwise making available for use of the objects</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p>	<p>designated in subparagraph 1.a.i., and also the production and procurement for use of the objects designated in subparagraph 1.a.ii of Article 6 of the Convention.</p>
<p><b>Title 2 – Computer-related offences</b></p>	
<p><b>Article 7 – Computer-related forgery</b>  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p>	<p><b>Criminal Code of Ukraine</b></p> <p><b>Article 361. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks</b></p> <p>1. Unauthorized interference in the operation of electronic computers, computer-based systems, computer networks or telecommunication networks, which resulted in the leak, loss, counterfeiting, blocking of information, troubling the processing of information or violating the established procedure for its routing, - shall be punishable by a fine in the amount of six hundred to one thousand non-taxable minimum incomes of citizens, or by restriction of freedom for a term of two to five years, or by imprisonment for a term up to three years, with or without deprivation of right to hold certain positions or engage in certain activities for a term up to two years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.</p> <p>2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a substantial damage, - shall be punishable by imprisonment for a term of three to six years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for unauthorized interference and which belong to the offender.</p> <p><b>Note.</b> Under Articles 361 – 363-1, it is understood that physical damage is considered to be substantial if its value one hundred times and more exceeds non-taxable minimum incomes of citizens.</p> <p><b>Article 362. Unauthorized actions with information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, such actions being committed by a person having the</b></p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p><b>right of access thereto</b></p> <p>1. Unauthorized alteration, deletion, or blocking of information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, such actions being committed by a person having the right of access thereto, - shall be punishable by a fine in the amount of six hundred to one thousand non-taxable minimum incomes of citizens, or by correctional works for a term up to two years, with confiscation of software and hardware which were used for unauthorized alteration, deletion, or blocking of information and which belong to the offender.</p> <p>2. Unauthorized interception or copying of information which is processed in electronic computers, computer-based systems, computer networks or stored on mediums carrying such information, if such actions resulted in the leak of the information and were committed by a person having the right of access thereto, - shall be punishable by imprisonment for a term up to three years, with deprivation of right to hold certain positions or engage in certain activities for the same term and with confiscation of software and hardware which were used for interception or copying of information and which belong to the offender.</p> <p>3. Actions as referred to in paragraph 1 or 2 of the present Article if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a large damage, - shall be punishable by imprisonment for a term of three to six years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years and with confiscation of software and hardware which were used for unauthorized actions with information and which belong to the offender.</p>
<p><b>Article 8 – Computer-related fraud</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <ul style="list-style-type: none"> <li>a any input, alteration, deletion or suppression of computer data;</li> <li>b any interference with the functioning of a computer system,</li> </ul>	<p><b>Criminal Code of Ukraine</b></p> <p><b>Article 190. Fraud</b></p> <p>1. Taking possession of someone else's property, or obtaining the property title by deceit or breach of confidence (fraud), - shall be punishable by a fine up to 50 tax-free minimum incomes, or correctional labor for a term up to two years, or restraint of liberty for a term up to three years.</p> <p>2. Fraud, if repeated, or committed by a group of persons upon their prior conspiracy, or where it caused significant damage to the victim, - shall be punishable by a fine of 50 to 100 tax-free minimum incomes, or correctional labor for a term of one to two years, or restraint of liberty for a term up to five</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	years, or imprisonment for a term up to three years. 3. Fraud committed in gross amounts or by unlawful operations involving computerized equipment, - shall be punishable by imprisonment for a term of three to eight years. 4. Fraud committed in an especially gross amount, or by an organized group, - shall be punishable by imprisonment for a term of eight to fifteen years and forfeiture of property.
<b>Title 3 – Content-related offences</b>	
<p><b>Article 9 – Offences related to child pornography</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <ul style="list-style-type: none"> <li>a producing child pornography for the purpose of its distribution through a computer system;</li> <li>b offering or making available child pornography through a computer system;</li> <li>c distributing or transmitting child pornography through a computer system;</li> <li>d procuring child pornography through a computer system for oneself or for another person;</li> <li>e possessing child pornography in a computer system or on a computer-data storage medium.</li> </ul> <p>2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:</p> <ul style="list-style-type: none"> <li>a a minor engaged in sexually explicit conduct;</li> <li>b a person appearing to be a minor engaged in sexually explicit conduct;</li> <li>c realistic images representing a minor engaged in sexually explicit conduct</li> </ul> <p>3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.</p> <p>4 Each Party may reserve the right not to apply, in whole or in part,</p>	<p><b>Reservation contained in the instrument of ratification deposited on 10 March 2006</b></p> <p>Ukraine reserves the right not to apply to the full extent subparagraphs 1.d and 1.e of Article 9 of the Convention.</p> <p><b>Article 301. Importation, making, sale or distribution of pornographic items</b></p> <p>1. Importation into Ukraine of images, works, or other items of pornographic character, for sale or distribution purpose, or making, transporting or otherwise moving for the same purpose, or sale or distribution thereof, and coercing others to participate in their making, - shall be punishable by a fine of 50 to 100 tax-free minimum incomes, or confinement for a term up to six months, or restraint of liberty for a term up to three years, with the forfeiture of pornographic images or other items and means of their making and distribution.</p> <p>2. The same actions committed in regard to pornographic motion pictures and video productions, computer programs, as well as the sale of pornographic images or other items to minors or disseminating such works, images and items among them, - shall be punishable by a fine of 100 to 300 tax-free minimum incomes, or restraint of liberty for a term up to five years, or imprisonment for the same term, with the forfeiture of pornographic motion pictures and video productions and means of their making and showing.</p> <p>3. Any such acts as provided for by paragraph 1 or 2 of this Article, if repeated, or committed by a group of persons upon their prior conspiracy, and</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.</p>	<p>also compelling minors to participate in the making of pornographic works, images, motion pictures, video films, or computer programs, - shall be punishable by imprisonment of three to seven years with the deprivation of the right to occupy certain positions or engage in certain activities for a term up to three years and forfeiture of pornographic items, motion pictures, video productions, computer programs, and means of their making, dissemination and showing.</p> <p>4. Acts provided by parts one or two of this article committed on works, images or other items of a pornographic nature containing child pornography or forcing minors to participate in the creation of works, images or film and video software pornography - punishable by imprisonment of five to ten years, with disqualification to hold certain positions or engage in certain activities for up to three years and forfeiture of pornographic materials, film and video material media software, means of production, distribution and showing.</p> <p>5. Actions provided by paragraph four of this article committed repeatedly or by prior agreement by a group of persons, or to obtain significant profits - punishable by imprisonment for a term of seven to twelve years with disqualification to hold certain positions or engage in certain activities for up to three years and forfeiture of pornographic materials, film and video material media software, means of production, distribution and demonstration.</p> <p><b>Note.</b> Receiving income on a large scale occurs when the amount equals or exceeds the tax-free minimum incomes.</p>
<p><b>Title 4 – Offences related to infringements of copyright and related rights</b></p>	
<p><b>Article 10 – Offences related to infringements of copyright and related rights</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the 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</p>	<p><b>Code of Ukraine on Administrative Offenses</b></p> <p><b>Article 51<sup>2</sup>. Violation of rights to object of intellectual property</b></p> <p>Illegal use of intellectual property (literary or artistic work, their performance, phonogram, broadcasting organization's transmission, computer programs, databases and scientific discovery, invention, utility model, industrial design, trademark, plant chips, innovations, plant varieties, etc.), assigning authorship on such objects or another intentional infringement of intellectual property rights object is protected by law -</p>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

wilfully, on a commercial scale and by means of a computer system.

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

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

entails a fine ranging from ten to two hundred times the income with seizure of illegally manufactured products and equipment and materials used for its production.

**Criminal Code of Ukraine****Article 176. Breach of copyright and related rights**

1. Illegal reproduction, distribution of scientific, literary, and art works, computer software or databases, as well as illegal reproduction, distribution of phonograms, videograms, and broadcast programs, their illegal duplication and distribution on audio and video tapes, disks, and other media, or any other willful breach of copyright and related rights if such actions caused a substantial physical damage, - shall be punishable by a fine in the amount of two hundred to one thousand non-taxable minimum incomes of citizens or by correctional works for a term up to two years, or by imprisonment for the same term, with the forfeiture and destruction of all copies of works, physical media, computer software, databases, performances, phonograms, videograms, broadcast programs, and of equipment and instruments and materials which were specifically used for the production of the same.

2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or where they caused a large physical damage, - shall be punishable by a fine in the amount of one to two thousand non-taxable minimum incomes of citizens or by correctional works for a term up to two years, or by imprisonment for a term of two to five years, with the forfeiture and destruction of all copies of works, physical media, computer software, databases, performances, phonograms, videograms, broadcast programs, and of equipment and instruments and materials which were specifically used for the production of the same.

3. Actions referred to in paragraphs 1 or 2 of the present Article if committed by an official with abuse of his position or by an organized group, or if such actions caused an especially large physical damage, - shall be punishable by a fine in the amount of two to three thousand non-taxable minimum incomes of citizens or by imprisonment for a term of three to six years, with or without deprivation of right to hold certain positions or engage in certain activities for a term of up to three years, with the forfeiture and destruction of all copies of works, physical media, computer

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

software, databases, performances, phonograms, videograms, broadcast programs, and of equipment and instruments and materials which were specifically used for the production of the same.

Note: In Articles 176 and 177 of the present Code, it is understood that physical damage is considered to be substantial if its amount twenty or more times exceeds non-taxable minimum income of citizens; large if its amount two hundred or more times exceeds non-taxable minimum income of citizens; especially large its amount one thousand or more times exceeds non-taxable minimum income of citizens.

**Article 229. Illegal use of a trade mark for goods and services, business name, qualified designation of the origin of goods**

1. Illegal use of a trade mark for goods and services, business name, qualified designation of the origin of goods, or any other wilful violation of the right to such assets if it caused substantial physical damage, - shall be punishable by a fine in the amount of two hundred to one thousand non-taxable minimum incomes of citizens or by correctional works for a term up to two years, or by imprisonment for the same term, with forfeiture of related products and equipment, and materials which were specifically used for the production thereof.

2. The same actions if repeated or committed by a group of individuals upon prior conspiracy, or if they caused a large physical damage, - shall be punishable by a fine in the amount of one thousand to two thousand non-taxable minimum incomes of citizens or by correctional works for a term up to two years, or by imprisonment for a term of two to five years, with forfeiture of related products and equipment, and materials which were specifically used for the production thereof.

3. Actions as referred to in paragraph 1 or 2 of the present Article if committed by an official through abuse of his position or by an organized group, or if they caused an especially large physical damage, - shall be punishable by a fine in the amount of two thousand to three thousand non-taxable minimum incomes of citizens or by imprisonment for a term of three to six years, with deprivation of right to hold certain positions or engage in certain activities for a term up to three years, with forfeiture of related products and equipment, and materials



BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>which were specifically used for the production thereof.</p> <p>Note. It is understood that physical damage is considered to be substantial if its value twenty and more times exceeds the level of non-taxable income of citizens; large if its value two hundred and more times exceeds the level of non-taxable income of citizens; especially large if its value one thousand and more times exceeds the level of non-taxable income of citizens.</p>
<b>Title 5 – Ancillary liability and sanctions</b>	
<p><b>Article 11 – Attempt and aiding or abetting</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	<p><b>Criminal Code of Ukraine</b></p> <p><b>Article 14. Preparation for crime</b></p> <p>1. The preparation for crime shall mean the looking out or adapting means and tools, or looking for accomplices to, or conspiring for, an offense, removing of obstacles to an offense, or otherwise intended conditioning of an offense.</p> <p>2. Preparation to commit a minor criminal offense does not give rise to criminal liability.</p> <p><b>Article 15. Criminal attempt</b></p> <p>1. A criminal attempt shall mean a directly intended act (action or omission) made by a person and aimed directly at the commission of a criminal offense prescribed by the relevant article of the Special Part of this Code, where this criminal offense has not been consummated for reasons beyond that person's control.</p> <p>2. A criminal attempt shall be consummated where a person has completed all such actions as he/she deemed necessary for the consummation of an offense, however, the offense was not completed for the reasons beyond that person's control.</p> <p>3. A criminal attempt shall be unconsummated where a person has not completed all such actions as he/she deemed necessary for the consummation of an offense for the reasons beyond that person's control.</p> <p><b>Article 16. Criminal liability for an unconsummated criminal offense</b></p>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

The criminal liability for the preparation for crime and a criminal attempt shall rise under Article 14 or 15 and that article of the Special Part of this Code which prescribes liability for the consummated crime.

**Article 26. The notion of complicity**

Criminal complicity is the wilful co-participation of several criminal offenders in an intended criminal offense.

**Article 27. Types of accomplices**

1. Organizer, abettor and accessory, together with the principal offender, are deemed to be accomplices in a criminal offense.
2. The principal (or co-principal) is the person who, in association with other criminal offenders, has committed a criminal offense under this Code, directly or through other persons, who cannot be criminally liable, in accordance with the law, for what they have committed.
3. The organizer is a person who has organized a criminal offense (or criminal offenses) or supervised its (their) preparation or commission. The organizer is also a person who has created an organized group or criminal organization, or supervised it, or financed it, or organized the covering up of the criminal activity of an organized group or criminal organization.
4. The abettor is a person who has induced any other accomplice to a criminal offense, by way of persuasion, subornation, threat, coercion or otherwise.
5. The accessory is a person who has facilitated the commission of a criminal offense by other accomplices, by way of advice, or instructions, or by supplying the means or tools, or removing obstacles, and also a person who promised in advance to conceal a criminal offender, tools or means, traces of crime or criminally obtained things, to buy or sell such things, or otherwise facilitate the covering up of a criminal offense.
6. The concealment of a criminal offender, tools or means of a criminal offense, traces of crime or criminally obtained things, or buying or selling such things shall not constitute complicity where they have not been promised in advance. Persons who have committed such acts shall be criminally liable only in cases prescribed by Articles 198 and 396 of this Code.
7. A promised failure to report a crime which is definitely known to be in

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>preparation or in progress, prior to the consummation of such, shall not constitute complicity. Any such person shall be criminally liable only if the act so committed comprises the elements of any other criminal offense.</p> <p><b>Article 29. Criminal liability of accomplices</b></p> <p>1. The principal (or co-principals) shall be criminally liable under that article of the Special Part of this Code which creates the offense he has committed.</p> <p>2. The organized, abettor and accessory shall be criminally liable under the respective paragraph of Article 27 and that article (or paragraph of the article) of the Special Part of this Code which creates an offense committed by the principal.</p> <p>3. The features of character of a specific accomplice shall be criminated only upon such accomplice. Other circumstances that aggravate responsibility and are provided for by articles of the Special Part of this Code as the elements of a crime that affect the treatment of the principal's actions, shall be criminated only upon the accomplice who was conscious of such circumstances.</p> <p>4. Where the principal commits an unconsummated criminal offense, other accomplices shall be criminally liable for complicity in an unconsummated crime.</p> <p>5. Accessories shall not be criminally liable for the act committed by the principal, where that act was no part of their intent.</p>
<p><b>Article 12 – Corporate liability</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:</p> <ul style="list-style-type: none"> <li>a a power of representation of the legal person;</li> <li>b an authority to take decisions on behalf of the legal person;</li> <li>c an authority to exercise control within the legal person.</li> </ul> <p>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the</p>	<p><i>n/a</i></p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>benefit of that legal person by a natural person acting under its authority.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	
<p><b>Article 13 – Sanctions and measures</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.</p> <p>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.</p>	Indicated above, in relation to criminal offences listed
<b><i>Section 2 – Procedural law</i></b>	
<p><b>Article 14 – Scope of procedural provisions</b></p> <p>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.</p> <p>2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <ul style="list-style-type: none"> <li>a the criminal offences established in accordance with Articles 2 through 11 of this Convention;</li> <li>b other criminal offences committed by means of a computer system; and</li> <li>c the collection of evidence in electronic form of a criminal offence.</li> </ul> <p>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</p>	Provided by the Code of Criminal Procedure, as listed below.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>referred to in Article 20.</p> <p>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:</p> <ul style="list-style-type: none"> <li>i is being operated for the benefit of a closed group of users, and</li> <li>ii does not employ public communications networks and is not connected with another computer system, whether public or private,</li> </ul> <p>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</p>	
<p><b>Article 15 – Conditions and safeguards</b></p> <p>1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.</p> <p>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.</p> <p>3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.</p>	<p><b>Criminal Procedure Code</b></p> <p><b>Article 7. General principles of criminal proceedings</b></p> <p>1. The matter and manner of criminal proceedings must conform to the general principles of criminal proceedings such as, but not limited to:</p> <ol style="list-style-type: none"> <li>1) the rule of law;</li> <li>2) legitimacy;</li> <li>3) equality before law and court;</li> <li>4) respect for human dignity;</li> <li>5) ensuring the right to liberty and security of person;</li> <li>6) inviolability of home or any other possession of a person;</li> <li>7) confidentiality of communication;</li> <li>8) non-interference in private life;</li> <li>9) security of the ownership right;</li> <li>10) presumption of innocence and conclusive proof of guilt;</li> <li>11) freedom from self-incrimination and the right to not testify against one’s close relatives and family members;</li> <li>12) prohibition of double jeopardy</li> <li>13) ensuring the right to defense;</li> <li>14) access to justice and the binding nature of court rulings;</li> <li>15) adversarial nature of parties, freedom to present their evidence to the court and prove the preponderance of this evidence before the court;</li> </ol>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

16) directness of examination of testimonies, objects and documents;  
 17) ensuring the right to challenge procedural decision, actions or inactivity;  
 18) publicity of criminal proceedings;  
 19) optionality of criminal proceedings  
 20) publicity and openness of judicial proceedings and their full recording using technical means;  
 21) reasonable time for criminal proceedings;  
 22) language of the criminal proceedings.  
 2. The list of principles of criminal proceedings set forth in this Chapter is not exhaustive.

**Article 8. Rule of law**

1. Criminal proceedings shall be conducted in accordance with the principle of the rule of law, under which a human being, his rights and freedoms are the highest values which define content and areas of State activities.  
 2. The principle of the rule of law in criminal proceedings shall be applied with due consideration of the practices of the European Court of Human Rights.

**Article 9. Legality**

1. During criminal proceedings, a court, investigating judge, public prosecutor, chief of pre-trial investigation agency, investigator, other officials of state authorities shall be required to steadfastly comply with the requirements of the Constitution of Ukraine, this Code, and international treaties the Verkhovna Rada of Ukraine has given its consent to be bound by, and requirements of other laws.  
 2. Prosecutor, chief of pre-trial investigation agency, investigator shall be required to examine comprehensively, fully and impartially the circumstances of criminal proceedings; find circumstances both of incriminating and exculpatory nature in respect of the suspect, the accused, as well as the circumstances mitigating and aggravating their punishment; make adequate legal evaluation thereof and ensure the adoption of lawful and impartial procedural decisions.  
 3. Laws and other legal regulatory acts of Ukraine, in so far as they relate to criminal proceedings, must be in line with this Code. No law contradicting this Code may

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

be applied in the conduct of criminal proceedings.

4. Wherever provisions of this Code contradict an international treaty the Verkhovna Rada of Ukraine has given its consent to be bound by, provisions of the relevant international treaty of Ukraine shall apply.

5. The criminal procedural legislation of Ukraine shall be applied in the light of the case law of the European Court for Human Rights.

6. Whenever provisions of the present Code do not regulate the matters of criminal proceedings or regulate such vaguely, the general principles of criminal proceedings as specified in paragraph one of Article 7 of this Code shall apply.

**Article 10. Equality before the law and the court**

1. Nobody may be given privilege or restricted in procedural rights as set forth in the present Code on the grounds of race, skin color, political, religious, or any other beliefs, sex, ethnic or social origin, property status, place of residence, nationality, education, occupation, as well as linguistic or any other grounds whatsoever.

2. In the course of criminal proceedings, in cases and according to the procedure stipulated by the present Code, certain categories of individuals (underage individuals, foreigners, mentally and physically disabled people, etc) shall have additional rights and guarantees.

**Article 11. Respect for human dignity**

1. In the course of criminal proceedings, respect for human dignity, rights, and freedoms of every person must be ensured.

2. In the course of criminal proceedings, it shall be prohibited to subject an individual to torture or to inhuman or degrading treatment or punishment, or to threaten or use such treatment, or to keep an individual in humiliating conditions, or to force to actions which humiliate dignity.

3. Everyone shall have the right to protect, by all means which are not prohibited by law, their dignity, rights, freedoms, and interests, which have been violated in the course of criminal proceedings.

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION****Article 12. Right to liberty and personal inviolability**

1. In the course of criminal proceedings, no one shall be kept into custody, be detained or

otherwise restrained in their right to freedom of movement upon criminal suspicion or charge

other than on grounds and according to the procedure specified in this Code.

2. Everyone who has been taken into custody or apprehended upon suspicion or charge of

having committed a criminal offence or otherwise deprived of liberty shall as soon as practicable

be brought before an investigating judge to decide on the lawfulness and reasonableness of their

detention, other deprivation of liberty and continued custody. The detained person shall be

promptly released from custody if within 72 hours from the moment of his detention he is not

served a reasoned court decision on keeping in custody.

3. A person's detention, taking into custody or other restraint in his right to freedom of

movement, as well as his location, must be immediately brought to notice, as provided herein, of

his close relatives, family members or other persons of such person's own choosing.

4. Anyone kept in custody or otherwise deprived of liberty in excess of the time prescribed

by this Code must be promptly released.

5. Where performed without grounds or in contravention of the procedure set forth in this

Code, a person's detention, taking into custody or other restraint of his right to freedom of

movement during the criminal proceedings shall entail a liability as provided by law.

**Article 13. Inviolability of home or other possession of a person**

1. Entering a home or any other possession of an individual, conducting inspection or

search therein shall not be allowed other than upon a reasoned court decision, except as

otherwise provided in this Code.



**BUDAPEST CONVENTION****DOMESTIC LEGISLATION****Article 14. Confidentiality of communication**

1. In the course of criminal proceedings, everyone shall be guaranteed confidentiality of correspondence, telephone conversations, cable, and other correspondence and other forms of communication.
2. Interference in the confidentiality of communication shall be possible only upon court's ruling in cases prescribed in the present Code, in view of preventing the commission of a crime of grave or especially grave severity, finding out its circumstances, and identifying the individual who committed the crime, if achieving this objective is impossible otherwise.
3. Information, which has been obtained as a result of interference in the confidentiality of communication, may not be used otherwise than for the purpose of criminal proceedings.

**Article 15. Non-interference in private life**

1. In the course of criminal proceedings, everyone shall be guaranteed non-interference in private (personal and family) life.
2. No one may collect, store, use and impart information on private life of an individual without their consent, except for cases prescribed in the present Code.
3. Information on private life of an individual obtained in accordance with the procedure established by the present Code may not be used otherwise than for the purpose of achieving the objectives of criminal proceedings.
4. Everyone who has been granted access to information on private life shall be required to prevent disclosure of such information.

**Article 16. Security of the ownership right**

1. In the course of criminal proceedings, deprivation or restriction of the right to ownership shall be made only upon a motivated court's decision adopted as prescribed in the present Code.
2. Temporary arrest of property without court decision shall be tolerated on grounds and

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

according to<sup>9</sup> the procedure prescribed in the present Code.

**Article 17. Presumption of innocence and conclusive proof of guilt**

1. An individual shall be considered innocent of the commission of a criminal offence and may not be imposed a criminal penalty unless their guilt is proved in accordance with the procedure prescribed in the present Code and is established in the court judgment of conviction which has taken legal effect.
2. No one shall be required to prove their innocence of having committed a criminal offence and shall be acquitted unless the prosecution proves their guilt beyond any reasonable doubt.
3. Suspicion, charges may not be based on evidence obtained illegally.
4. Any doubt as to the proof of the guilt of an individual shall be interpreted in this person's favor.
5. A person whose criminal guilt has not been found in a valid judgement of conviction shall be treated as an innocent one.

**Article 18. Freedom from self-incrimination; Right to not testify against close relatives and family members**

1. No one shall be compelled to admit their guilt of a criminal offence or to give explanations, testimonies, which may serve a ground for suspecting them or charging with a commission of a criminal offence.
2. Everyone shall have the right to keep silence about suspicion, a charge against him or waive answering questions at any time, and, also, to be promptly informed of such right.
3. No person may be compelled to give any explanations or testimonies, which may serve a ground for suspecting his close relatives or family members of, or charging them with, commission of a criminal offence.

**Article 19. Prohibition of double jeopardy**

1. No one may be charged with, or punished twice for, a criminal offence, for

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

which he was acquitted or convicted by a valid judgment.

2. Criminal proceedings shall be subject to immediate termination when it becomes known of a valid judgment delivered on the same charge.

**Article 20. Right to defense**

1. A suspect, an accused, acquitted or a convicted person shall have the right to defense consisting in the opportunity to give oral or written explanations in respect of the suspicion or accusation, collect and produce evidence, attend the criminal proceedings personally, as well as benefit from legal assistance of a defense counsel, as well as exercise other procedural rights as set forth in this Code.

2. Investigator, public prosecutor, investigating judge, and court shall be required to advise the suspect, the accused of their rights and ensure their right to a competent legal assistance by a defense counsel whom they select or appoint on their own.

3. Legal assistance to a suspect, an accused shall be provided at no cost at the expense of the state in cases specified by the present Code and/or the law, which regulates provision of legal assistance at no cost.

4. Participation of a defense counsel of the suspect, the accused in criminal proceedings shall not affect their procedural rights.

**Article 21. Access to justice and the binding nature of court rulings**

1. Everyone shall be guaranteed the right to a fair trial and resolution of the case within reasonable time limits by independent and impartial court established on the basis of law.

2. Court's judgment or ruling that took legal effect as prescribed by the present Code shall be binding and subject to unconditional execution in the entire territory of Ukraine.

3. Everyone has the right to participate in any judicial hearings of the matter related to their

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>rights and duties in accordance with the procedure set forth in the present Code.            4. Unless otherwise prescribed by in the present Code, conducting criminal proceedings may not be an obstacle to a person's access to any other legal remedies to protect their rights in case where in the course of the criminal proceedings their rights enshrined in the Constitution of Ukraine and international treaties of Ukraine are being infringed.</p>
<p><b>Article 16 – Expedited preservation of stored computer data</b>            1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.</p> <p>2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Criminal Procedure Code</b></p> <p><b>Article 159. General provisions for provisional access to objects and documents</b>            1. Provisional access to objects and documents consists in providing a party in criminal proceedings by the person who owns such objects and documents, with the opportunity to examine such objects and documents, make copies thereof and, upon adoption of the appropriate ruling by investigating judge, court, seize them (execute seizure).            2. Provisional access to objects and documents shall be executed based on a ruling of investigating judge, court.</p> <p><b>Article 160. Motion to grant provisional access to objects and documents</b>            1. Parties to criminal proceedings may apply to investigating judge during pre-trial investigation or to court during trial, for granting provisional access to objects and documents of criminal proceedings, except those specified in Article 161 of the present Code. Investigator may submit such motion upon approval of public prosecutor.            2. A motion shall contain:            1) brief description of circumstances of the criminal offense in connection with which the motion is filed;            2) legal qualification of the criminal offense under Ukrainian law on criminal liability indicating the article (paragraphs of article);            3) objects and documents the provisional access to which is planned to be granted;</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>4) grounds to believe that the objects and documents are or can be in possession of the physical or legal person concerned;</p> <p>5) significance of the objects and documents for establishing circumstances in the criminal proceedings concerned;</p> <p>6) possibility to use as evidence the information contained in the objects and documents, and impossibility to otherwise prove circumstances which are supposed to be proved with the use of such objects and documents, in case the motion to grant provisional access pertains to objects and documents containing secrets protected by law;</p> <p>7) substantiation of the necessity to seize the objects and documents, if such an issue is raised by a party to criminal proceedings.</p>
<p><b>Article 17 – Expedited preservation and partial disclosure of traffic data</b></p> <p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <p>a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and</p> <p>b ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><i>n/a</i></p>
<p><b>Article 18 – Production order</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and</p> <p>b a service provider offering its services in the territory of the Party to</p>	<p><b>Criminal Procedure Code</b></p> <p><b>Article 159. General provisions for provisional access to objects and documents</b></p> <p>1. Provisional access to objects and documents consists in providing a party in criminal proceedings by the person who owns such objects and documents, with the</p>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

submit subscriber information relating to such services in that service provider's possession or control.

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

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

- a the type of communication service used, the technical provisions taken thereto and the period of service;
- b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
- c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

opportunity to examine such objects and documents, make copies thereof and, upon adoption of the appropriate ruling by investigating judge, court, seize them (execute seizure).  
2. Provisional access to objects and documents shall be executed based on a ruling of investigating judge, court.

**Article 160. Motion to grant provisional access to objects and documents**

1. Parties to criminal proceedings may apply to investigating judge during pre-trial investigation or to court during trial, for granting provisional access to objects and documents of criminal proceedings, except those specified in Article 161 of the present Code. Investigator may submit such motion upon approval of public prosecutor.  
2. A motion shall contain:

- 1) brief description of circumstances of the criminal offense in connection with which the motion is filed;
- 2) legal qualification of the criminal offense under Ukrainian law on criminal liability indicating the article (paragraphs of article);
- 3) objects and documents the provisional access to which is planned to be granted;
- 4) grounds to believe that the objects and documents are or can be in possession of the physical or legal person concerned;
- 5) significance of the objects and documents for establishing circumstances in the criminal proceedings concerned;
- 6) possibility to use as evidence the information contained in the objects and documents, and impossibility to otherwise prove circumstances which are supposed to be proved with the use of such objects and documents, in case the motion to grant provisional access pertains to objects and documents containing secrets protected by law;
- 7) substantiation of the necessity to seize the objects and documents, if such an issue is

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p><b>Article 19 – Search and seizure of stored computer data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <p style="padding-left: 20px;">a a computer system or part of it and computer data stored therein; and</p> <p style="padding-left: 20px;">b a computer-data storage medium in which computer data may be stored</p> <p style="padding-left: 40px;">in its territory.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.</p> <p>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:</p> <p style="padding-left: 20px;">a seize or similarly secure a computer system or part of it or a computer-data storage medium;</p> <p style="padding-left: 20px;">b make and retain a copy of those computer data;</p> <p style="padding-left: 20px;">c maintain the integrity of the relevant stored computer data;</p> <p style="padding-left: 20px;">d render inaccessible or remove those computer data in the accessed computer system.</p> <p>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.</p> <p>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>raised by a party to criminal proceedings.</p> <p><b>Criminal Procedure Code</b></p> <p><b>Article 234. Search</b></p> <p>1. A search is conducted with the purpose of finding and fixing information on circumstances of commission of criminal offense, finding tools of criminal offense or property obtained as a result of its commission, as well as of establishing the whereabouts of wanted persons.</p> <p>2. A search shall be based on investigating judge’s ruling.</p> <p>3. Whenever it is necessary to conduct a search, investigator with approval of public prosecutor, or public prosecutor shall submit an appropriate request to investigating judge containing the following information:</p> <p>1) designation and registration number of criminal proceedings;</p> <p>2) brief description of circumstances of the criminal offense in connection with investigating which the request is submitted;</p> <p>3) legal qualification of the criminal offense indicating Article (Article part) of the Ukrainian law on criminal liability;</p> <p>4) grounds for search;</p> <p>5) home or any other possession of a person or a part thereof or other possession of the person where the search should be conducted;</p> <p>6) person who owns the home or other possession, and person in whose actual possession it actually is;</p> <p>7) objects, documents or individuals to be found.</p> <p>The request shall be required to be attached originals or copies of documents and other materials by which public prosecutor, investigator substantiates the arguments of the request, as well as an extract from the Integrated Register of Pre-Trial Investigations related to the criminal proceedings in the framework of which the request is submitted.</p> <p>4. A request for search shall be considered in court on the day of receipt, with participation of investigator or public prosecutor.</p> <p>5. Investigating judge shall reject a request for search unless public prosecutor, investigator</p>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

proves the existence of sufficient grounds to believe that:

- 1) a criminal offense was committed;
- 2) objects and documents to be found are important for pre-trial investigation;
- 3) knowledge contained in objects and documents being searched may be found to be evidence during trial;
- 4) objects, documents or persons to be found are in the home or any other possession of a person indicated in the request.

**Article 235. Ruling to authorize a search of home or any other possession of a person**

1. Investigating judge's ruling authorizing search of home or other possession of a person on grounds provided in public prosecutor's, investigator's request, shall give the right to enter home or other possession of a person only once.
2. Investigating judge's ruling authorizing search of home or other possession of a person shall be required to comply with general requirements for court decisions laid down in the present Code as well as contain information on the following:
  - 1) term of effect of the ruling which may not exceed one month after the day it was passed;
  - 2) public prosecutor, investigator who requests the search;
  - 3) legal provision based on which the ruling is passed;
  - 4) home or any other possession of a person or a part thereof, or other possession of the person where the search should be conducted;
  - 5) person who owns the home or other possession, and person in whose actual possession it actually is;
  - 6) objects, documents or individuals to be found.
3. Two copies of the ruling should be prepared and expressly marked as copies.

**Article 236. Execution of the ruling to authorize search of home or any other possession of a person**

1. Investigator or public prosecutor may execute the ruling to authorize a search of home or any other possession of a person. The victim, the suspect, defense counsel,



**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

representative, and other participants to criminal proceedings may be invited to attend. Whenever investigator, public prosecutor needs assistance in issues requiring special knowledge, they may invite specialists to participate in the search. The investigator, public prosecutor shall take adequate measures to ensure that persons whose rights and legitimate interests may be abridged or violated are present during such search.

2. A search of home or other possession of a person based on investigating judge's ruling should be conducted in time when the least damage is caused to usual occupations of their owner unless the investigator, public prosecutor finds that meeting such requirement can seriously compromise the objective of the search.

3. Prior to the execution of investigating judge's ruling, the owner of home or any other possession or any other present individual in case of the absence of the owner, should be produced court's ruling and given a copy thereof. Investigator, public prosecutor may prohibit any person from leaving the searched place until the search is completed and from taking any action which impede conducting search. Failure to follow these requests entails liability established by law.

4. If no one is present in the home or other possession, the copy of ruling should be left visible in the home or other possession. In such a case, investigator, public prosecutor is required to ensure preservation of property contained in the home or any other possession and make it impossible for unauthorized individuals to have access thereto.

5. Search based on court's ruling should be conducted within the scope necessary to attain the objective of search. Upon decision of the investigator, public prosecutor, individuals present in the home or other possession may be searched if there are sufficient grounds to believe that

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

they hide on their person objects or documents which are important for criminal proceedings.

Such search should be conducted by individuals of the same sex.

6. During the search, investigator, public prosecutor shall have the right to open closed

premises, depositories, objects if the person present during the search, refuses to open them, or if

the search is conducted in the absence of persons specified in part three of this Article.

7. During the search, investigator, public prosecutor may conduct measurements, shoot

pictures, make audio or video recording, draw plans and schemes, produce graphic images of the

searched home or other possession of a person, or of particular objects, make prints and moulds,

inspect and seize objects and documents which are important for criminal proceedings. Objects

seized by law from circulation shall be subject to seizure irrespective of their relation to the

criminal proceedings concerned. Seized objects and documents not included in the list of those

directly allowed to be found in the ruling authorizing the search, and are not among objects

withdrawn by law from circulation, shall be deemed provisionally seized property.

8. Persons who are present during the search have the right to make statements in the

course of investigative (detective) action, such statements being entered in the record of search.

**Article 237. Inspection**

1. Investigator, public prosecutor shall carry out visual inspection of the area, premises,

items and documents to find and record the information relating to the commission of a criminal offence.

2. Inspection of home or any other possession of a person shall be done in accordance with

rules of the present Code governing the search of home or any other possession of a person.

3. The victim, suspect, defense counsel, legal representative and other

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>participants to criminal proceedings may be invited to take part in the inspection. In order to have assistance in matters requiring special knowledge, investigator, public prosecutor may invite specialist to participate in the inspection.</p> <p>4. Persons who are present during the inspection have the right to make statements in the course of investigative (detective) action, such statements being entered in the record of inspection.</p> <p>5. During inspection, it shall be allowed to seize only objects and documents of importance for the pre-trial investigation, and objects withdrawn from circulation. All objects and documents which have been seized are subject to immediate inspection and sealing with signed acknowledgement by participants to the inspection. If it is impossible to inspect objects and documents on the premises or if their inspection is complicated, they shall be temporarily sealed and stored as they are until final inspection and sealing thereof is made.</p> <p>6. Investigator, public prosecutor may prohibit any individual from leaving the inspected place till the completion of inspection and from committing any actions which impede inspection. Failure to comply with such requests entails liability under law.</p> <p>7. During inspection, investigator, public prosecutor or upon their assignment, the invited specialist may carry out measurements, photographing, audio or video recording, draw up plans and schemes, prepare graphical images of the place or particular objects, produce prints and moulds, examine and seize objects and documents of importance for criminal proceedings. Objects seized from circulation by law shall be subject to seizure irrespective of their relation to criminal proceedings. Seized objects and documents which are not objects seized from circulation by law shall be deemed provisionally seized property.</p>
<b>Article 20 – Real-time collection of traffic data</b>	<b>Law of Ukraine On Telecommunications</b>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

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

- a collect or record through the application of technical means on the territory of that Party, and
- b compel a service provider, within its existing technical capability:
  - i to collect or record through the application of technical means on the territory of that Party; or
  - ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

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

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

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

**Article 41. Liability of Telecommunication Operators/providers**

1. Telecommunication operators shall bear material liability before consumers for a failure to provide or undue provision of telecommunication services to the following extents:

- 1) for a failure to provide telecommunication services or provision of same in the volume being below the paid volume – the amount of the paid cost of the outstanding services plus a fine in the amount of 25 percent of the cost of the service;
- 2) for the delay with a telegram transmission leading to a failure to hand it or delayed handing it to a recipient – a fine in the amount of 50 percent of the cost of the paid service, as well as the refund to the consumer of the amount received for the service;
- 3) for the ungrounded disconnection of terminal equipment – in the amount of a subscription fee for the entire period of disconnection;
- 4) for the ungrounded reduction or modification of the services list – in the amount of a monthly f subscription fee;
- 5) in all other cases – in the amounts provided under the agreement on telecommunication services provision;
- 6) in case of failure to remedy, within 24 hours following the fixed time of the consumer's filing of an application to the effect of a telecommunication network damaging, disabling the consumer's access to the service or deterioration down to inadmissible values of quality indicators of a telecommunication service, the subscription fee for the entire period of damage shall not be calculated while the operator shall be obliged to, in the event of failure to remedy the damage within five days following the fixed time of the consumer's filing of a respective application, pay to a consumer a fine in the amount of 25 percent of the daily subscription fee for each day in excess of this term, being however not more than three month.

2. Telecommunication operators/providers shall not bear material liability before telecommunication services consumers for the failure to perform or undue performance of their respective obligations with respect to telecommunication services provision due

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

to circumstances beyond their control (earthquake, floods, tornados, etc.), theft or damage by perpetrators of line and station structures used by a telecommunication operator or through consumers default in cases provided for herein.

3. The matters involving the compensation of actual losses, moral damage, lost profit suffered as a result of the telecommunications operators/providers failure to meet their obligations under agreements shall be hear in a due course of law.

4. Telecommunications operators/providers shall not be held liable for the content of information transmitted through their networks.

**Criminal Procedure Code****Article 263. Collecting information from transport telecommunication networks**

1. Collecting information from transport telecommunication networks (networks which provide transmitting of any signs, signals, written texts, images and sounds or messages between telecommunication access networks connected) is a variety of interference in private communication conducted without the knowledge of individuals who use telecommunication facility for transmitting information based on the ruling rendered by the investigating judge, if there is possibility to substantiate the facts during its conducting, which have the importance for criminal proceedings.

2. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics which will allow to uniquely identify the subscriber under surveillance, transport telecommunication network, and terminal equipment which can be used for interference in private communication.

3. Collecting information from transport telecommunication networks means the conducting using appropriate watch facility the surveillance, selection and

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

recording information which is transmitted by an individual and have the importance for pre-trial investigation and also receiving, transformation and recording signals of different types which are transmitted by communication channels.

4. Collecting information from transport telecommunication networks is made by responsible units of the bodies of internal affairs and bodies of security. Managers and employees of telecommunication networks' operators shall be required to facilitate conducting the actions on collecting information from transport telecommunication networks, taking required measures in order not to disclose the fact of conducting such actions and the information obtained, and to preserve it unchanged.

**Article 264. Collecting information from electronic information systems**

1. Search, detection, and recording information stored in an electronic information system or any part thereof, access to the information system or any part thereof, as well as obtainment of such information without knowledge of its owner, possessor or keeper may be made based on the ruling rendered by the investigating judge, if there is information that such information system or any part thereof contains information of importance for a specific pre-trial investigation.

2. Obtainment of information from electronic information systems or parts thereof the access to which is not restricted by the system's owner, possessor or keeper, or is not related to circumventing a system of logical protection, shall not require permission of investigating judge.

3. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics of the electronic

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>information system which can be used for interference in private communication.</p> <p><b>Article 265. Recording and preserving information obtained from communication channels through the use of technological devices and as a result of collecting information from electronic information systems</b></p> <p>1. Contents of information which is transmitted by persons via the transport telecommunication networks shall be stated in the record of conducting of the said covert investigative (detective) actions. If such information is found to contain knowledge of importance for a specific pre-trial investigation, the record should reproduce its respective part, and then public prosecutor shall take measures to preserve information obtained by monitoring.</p> <p>2. Contents of information obtained as a result of monitoring an information system or any part thereof, shall be recorded on the appropriate medium by the individual who has been responsible for monitoring and who is required to ensure processing, preserving, and transmitting the information.</p>
<p><b>Article 21 – Interception of content data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:</p> <p>a collect or record through the application of technical means on the territory of that Party, and</p> <p>b compel a service provider, within its existing technical capability:</p> <p>    i to collect or record through the application of technical means on the territory of that Party, or</p> <p>    ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure</p>	<p><b>Criminal Procedure Code</b></p> <p><b>Article 258. General provisions related to interference in private communication</b></p> <p>1. Nobody may be subjected to interference in private communication without investigating judge’s ruling.</p> <p>2. Public prosecutor, investigator upon approval of public prosecutor shall be required to apply to investigating judge for permission to interfere in private communication as prescribed in Articles 246, 248-250 of the present Code, if any investigative (detective) action implies such interference.</p> <p>Whenever investigating judge passes the ruling to deny interference in private</p>

**BUDAPEST CONVENTION**

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.

**DOMESTIC LEGISLATION**

communication, public prosecutor, investigator may file a new request only with new information.

3. Communication is transmitting information in any way from one person to another directly or using any connection. Communication is considered to be private insofar as

information is transmitted and stored under such physical or legal conditions where participants to the communication can expect that such information is protected from interference on the part of others.

4. Interference in private communication implies access to the contents of communication under conditions when participants to the communication can reasonably expect that their communication is private. The following shall be types of interference in private communication:

- 1) audio, video monitoring of an individual;
- 2) arrest, examination and seizure of correspondence;
- 3) collecting information from telecommunication networks;
- 4) collecting information from electronic information systems.

5. Interference in private communication of defense counsel, between clergyman and the suspect, accused, convict, acquitted shall be forbidden.

**Article 262. Inspection and seizure of correspondence**

1. Seized correspondence shall be inspected in the postal office, which was assigned control and seizure of this correspondence, with participation of this office's representative and, in case of need, of a specialist. In the presence of the said individuals, investigator decides on the opening of correspondence and inspects seized correspondence.

2. Should objects (inclusive of substances), documents be found in the correspondence that are important for a certain pre-trial investigation, investigator within the scope prescribed in the



**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

investigating judge's ruling, shall conduct seizure of the correspondence concerned or limit himself to making copies or taking samples of relevant messages. Copies are made or samples taken in view of protecting confidentiality of correspondence arrest. If necessary, the person who inspects mail and cable correspondence, may take a decision to put special marks on the detected objects and documents, equip them with technical control devices, replace objects and substances which endanger surrounding people or are prohibited from being in free circulation, with their safe analogues.

3. If objects or documents of importance for pre-trial investigation are not found in the correspondence, investigator shall give instruction to deliver the correspondence inspected to the addressee.

4. A record shall be drawn up of each occurrence of inspection, seizure or arrest of correspondence as prescribed in the present Code. The record should necessarily state what kind of messages have been inspected, what has been seized from the messages, and what should be delivered to the addressee or temporarily kept, and from what messages copies or samples have been made, and the conduct of other actions as provided for in part two of this Article.

5. Managers and employees of postal offices shall be required to facilitate conducting this covert investigative (detective) action and not to disclose the fact of conducting this covert investigative (detective) action or the information obtained.

**Article 263. Collecting information from transport telecommunication networks**

1. Collecting information from transport telecommunication networks (networks which

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

provide transmitting of any signs, signals, written texts, images and sounds or messages between telecommunication access networks connected) is a variety of interference in private communication conducted without the knowledge of individuals who use telecommunication facility for transmitting information based on the ruling rendered by the investigating judge, if there is possibility to substantiate the facts during its conducting, which have the importance for criminal proceedings.

2. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics which will allow to uniquely identify the subscriber under surveillance, transport telecommunication network, and terminal equipment which can be used for interference in private communication.

3. Collecting information from transport telecommunication networks means the conducting using appropriate watch facility the surveillance, selection and recording information which is transmitted by an individual and have the importance for pre-trial investigation and also receiving, transformation and recording signals of different types which are transmitted by communication channels.

4. Collecting information from transport telecommunication networks is made by responsible units of the bodies of internal affairs and bodies of security. Managers and employees of telecommunication networks' operators shall be required to facilitate conducting the actions on collecting information from transport telecommunication networks, taking required measures in order not to disclose the fact of conducting such actions and the information obtained, and to preserve it unchanged.

**Article 264. Collecting information from electronic information systems**

[Back to the Table of Contents](#)

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

1. Search, detection, and recording information stored in an electronic information system or any part thereof, access to the information system or any part thereof, as well as obtainment of such information without knowledge of its owner, possessor or keeper may be made based on the ruling rendered by the investigating judge, if there is information that such information system or any part thereof contains information of importance for a specific pre-trial investigation.

2. Obtainment of information from electronic information systems or parts thereof the access to which is not restricted by the system's owner, possessor or keeper, or is not related to circumventing a system of logical protection, shall not require permission of investigating judge.

3. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics of the electronic information system which can be used for interference in private communication.

**Article 265. Recording and preserving information obtained from communication channels through the use of technological devices and as a result of collecting information from electronic information systems**

1. Contents of information which is transmitted by persons via the transport telecommunication networks shall be stated in the record of conducting of the said covert investigative (detective) actions. If such information is found to contain knowledge of importance for a specific pre-trial investigation, the record should reproduce its respective part, and then public prosecutor shall take measures to preserve information obtained by monitoring.

2. Contents of information obtained as a result of monitoring an information system or any part thereof, shall be recorded on the appropriate medium by the individual who has been

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	responsible for monitoring and who is required to ensure processing, preserving, and transmitting the information.
<b>Section 3 – Jurisdiction</b>	
<p><b>Article 22 – Jurisdiction</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:</p> <ol style="list-style-type: none"> <li>a in its territory; or</li> <li>b on board a ship flying the flag of that Party; or</li> <li>c on board an aircraft registered under the laws of that Party; or</li> <li>d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.</li> </ol> <p>2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.</p> <p>3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.</p> <p>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.</p>	<p>According to Article 6 of the UA-CC persons who committed crimes on the territory of Ukraine, shall be criminally liable under this Code.</p> <p>A crime is committed on the territory of Ukraine if it has been initiated, continued, completed or discontinued on the territory of Ukraine.</p> <p>A crime is committed on the territory of Ukraine if it or at least one of the participants acted in Ukraine.</p> <p>The question of criminal liability of diplomatic representatives of foreign states and other citizens under the laws of Ukraine and international treaties ratified by the Verkhovna Rada of Ukraine is not a defendant in criminal courts Ukraine, if they commit a crime on the territory of Ukraine resolved diplomatically by.</p> <p>It should be noted that in Ukraine are equal:</p> <ul style="list-style-type: none"> <li>- military ships or boats flying the flag of Ukraine, regardless of whether they are at sea, in the territorial waters of another state or a foreign port;</li> <li>- the military air facilities are located in any place outside the airspace of Ukraine;</li> <li>- non-military ships or boats that are assigned to ports in Ukraine and flying the flag of Ukraine on the high seas;</li> <li>- non-military air facilities registered in Ukraine, which are in open airspace.</li> </ul> <p>According to Article 7 of the Criminal Code Ukraine nationals and stateless persons permanently residing in Ukraine who have committed crimes abroad shall be criminally liable under this Code, unless otherwise provided by international treaties of Ukraine ratified by the Verkhovna Rada of Ukraine .</p> <p>If the persons mentioned in the first paragraph of this article, committed crimes experienced criminal penalties outside Ukraine, they can not be held in Ukraine</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>criminal responsibility for these crimes.</p> <p>According to Article 8 of the UA-CC foreigners or stateless persons not residing permanently in Ukraine who have committed crimes abroad, subject to Ukraine liability under this Code in cases stipulated by international treaties or if they are committed by this Code grave or especially grave crimes against the rights and freedoms of citizens of Ukraine or the interests of Ukraine.</p> <p>According to Article 10 of the Criminal Code Ukraine nationals and stateless persons permanently residing in Ukraine who have committed crimes outside Ukraine may not be extradited to a foreign state for criminal prosecution and committal for trial.</p> <p>Foreigners who have committed crimes on the territory of Ukraine and convicted them on the basis of this Code may be transferred to serve his sentence for the offense that State of which they are, if the transfer provided by international treaties of Ukraine.</p> <p>Foreigners and stateless persons who permanently reside in Ukraine who have committed crimes outside Ukraine and within its territory may be extradited to a foreign state for criminal prosecution and committal for trial or transferred to serve his sentence if such issuance or transfer provided for in international treaties of Ukraine.</p>
<b>Chapter III – International co-operation</b>	
<p><b>Article 24 – Extradition</b></p> <p>1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.</p> <p>b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty</p>	<p><b>Criminal Procedure Code</b></p> <p><b>Article 573. Submitting a request for extradition</b></p> <p>1. A request for extradition may be submitted only provided that at least one of the offenses for which an extradition is requested may be punished with at least one year imprisonment or a person was sentenced to serve the punishment in the form of imprisonment and the unserved portion of sentence is at least four months.</p> <p>2. A request from a foreign competent authority for extradition may be considered only</p>

**BUDAPEST CONVENTION**

provided for under such arrangement or treaty shall apply.

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

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

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

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

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

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

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

**DOMESTIC LEGISLATION**

provided that all of the requirements specified in paragraph 1 of this article are met.

3. Requests for temporary extradition and transit shall be submitted and considered in accordance with the same procedures that apply to requests for extradition. When considering requests from foreign competent authorities for transit, extradition examination shall apply only to circumstances specified in article 589, paragraphs 1 and 2 of this Code.

4. A central authority of Ukraine may refuse to send the request to a foreign state if circumstances referred to in the present Code or the international treaty of Ukraine and which may preclude extradition, do exist. It may also refuse to grant permission to the competent authority of Ukraine to apply to a foreign state, if the extradition would be obviously unjustified based on the correlation between the severity of the criminal offence committed by the person, and the potential expenses required for the extradition.

**Article 574. Central authority of Ukraine for extradition**

1. Unless otherwise specified by the international treaty of Ukraine, central authorities of Ukraine for extradition shall respectively be the Prosecutor General's Office and the Ministry of Justice of Ukraine.

2. The Prosecutor General's Office shall be the central authority responsible for extradition of suspects or the accused in criminal proceedings during the pre-trial investigation.

3. The Ministry of Justice of Ukraine shall be the central authority responsible for extradition of defendants or the convicted in criminal proceedings during the court trial or the execution of a sentence.

4. In accordance with this Code, central authorities of Ukraine for extradition shall:

- 1) make requests to foreign competent authorities for extradition, temporary extradition or transit of a person;
- 2) consider and decide on requests from foreign competent authorities for

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>extradition, temporary extradition or transit of a person; 3) arrange extradition examinations; 4) arrange intake and referral of persons to be extradited, temporarily extradited or transited; 5) exercise other powers established by this article or an international agreement on extradition.</p> <p>During the stage of pre-trial investigation, the Prosecutor General's Office (Department for International Legal Cooperation and European Integration) is the central authority. At the trial stage, the Ministry of Justice (Division on Mutual Legal Assistance in Criminal Matters, International Legal Cooperation Department, Directorate for International Law) is handling MLA requests.</p>
<p><b>Article 25 – General principles relating to mutual assistance</b></p> <p>1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.</p> <p>2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.</p> <p>3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.</p> <p>4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the</p>	<p><b>Criminal Procedure Code</b></p> <p><b>Article 542. Scope of international cooperation in criminal proceedings</b></p> <p>1. International cooperation in criminal proceedings shall be the taking of measures necessary in order to provide international legal assistance through serving documents, conducting certain procedural actions, extradition of individuals who have committed criminal offences, provisional transfer of persons, taking over of criminal prosecution, transfer of sentenced persons, and enforcement of sentences. An international treaty of Ukraine may provide for other forms of cooperation in criminal proceedings than are specified in this Code.</p> <p><b>Article 543. Legislation which governs international cooperation in criminal proceedings</b></p> <p>1. This Code and effective international treaties of Ukraine shall specify the way in which the designated (central) authority of Ukraine shall forward requests to another state, consider requests for legal assistance from another state or an international judicial institution, and the</p>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

ground that the request concerns an offence which it considers a fiscal offence.

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

way in which such requests should be executed.

**Article 544. Providing and receiving international legal assistance or other international cooperation without a treaty**

1. In the absence of an international treaty of Ukraine, international legal assistance or any other cooperation may be provided upon the request from another state, or requested on the basis of reciprocity.
2. Designated (central) authority of Ukraine, when forwarding a request to such state, shall guarantee, in written form, to the requested Party that in future, such State's request for international legal assistance of the same type shall be considered.
3. Under provisions of part one of this Article, the designated (central) authority of Ukraine shall consider request of a foreign State only if the requesting State has guaranteed, in written form, to receive and consider, in future, Ukraine's request on the basis of reciprocity.
4. Designated (central) authority of Ukraine, when requesting international legal assistance from such state and providing international legal assistance thereto, shall be guided by the this Code.
5. In the absence of an international treaty with the state concerned, the designated (central) authority of Ukraine shall forward request for international legal assistance to the Ministry of foreign affairs of Ukraine, for subsequent transmitting it to the competent authority of the requested state via diplomatic channels.

**Article 545. Central authority of Ukraine**

1. The Prosecutor-General's Office of Ukraine shall make requests for international legal assistance in criminal proceedings during a pre-trial investigation and consider similar requests from foreign competent authorities, except pre-trial investigation of criminal offences referred to investigative jurisdiction of Anti-Corruption Bureau of Ukraine that in such cases



BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>performs functions of central authority of Ukraine.</p> <p>2. The Ministry of Justice of Ukraine shall refer requests from courts for international legal assistance in criminal proceedings during a court trial and consider similar requests from courts in foreign states.</p> <p>3. Where this Code or an effective international treaty of Ukraine prescribes a different procedure for relations, powers specified in paragraphs one and two of this Article shall extend to the body specified in those legislative acts.</p> <p>According to the newly adopted legislation the National Anticorruption Bureau of Ukraine is also a central authority in execution of the MLA requests at the stage of pre-trial investigation.</p>
<p><b>Article 26 – Spontaneous information</b></p> <p>1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.</p> <p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	
<p><b>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</b></p> <p>1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and</p>	<p><b>Criminal Procedure Code</b></p> <p><b>Article 544. Providing and receiving international legal assistance or other international cooperation without a treaty</b></p>

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

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

b The central authorities shall communicate directly with each other;

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

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

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

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

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

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

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

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

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

1. In the absence of an international treaty of Ukraine, international legal assistance or any other cooperation may be provided upon the request from another state, or requested on the basis of reciprocity.

2. Designated (central) authority of Ukraine, when forwarding a request to such state, shall guarantee, in written form, to the requested Party that in future, such State's request for international legal assistance of the same type shall be considered.

3. Under provisions of part one of this Article, the designated (central) authority of Ukraine shall consider request of a foreign State only if the requesting State has guaranteed, in written form, to receive and consider, in future, Ukraine's request on the basis of reciprocity.

4. Designated (central) authority of Ukraine, when requesting international legal assistance from such state and providing international legal assistance thereto, shall be guided by the this Code.

5. In the absence of an international treaty with the state concerned, the designated (central) authority of Ukraine shall forward request for international legal assistance to the Ministry of foreign affairs of Ukraine, for subsequent transmitting it to the competent authority of the requested state via diplomatic channels.

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

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:

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

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**

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

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

a the authority seeking the preservation;

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

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

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

e the necessity of the preservation; and

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

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

4 A Party that requires dual criminality as a condition for responding to

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

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

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

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

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

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

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

**Article 30 – Expedited disclosure of preserved traffic data**

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

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

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

b the requested Party considers that execution of the request is likely to

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.	
<p><b>Article 31 – Mutual assistance regarding accessing of stored computer data</b></p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p> <p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <ul style="list-style-type: none"> <li>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</li> <li>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</li> </ul>	
<p><b>Article 32 – Trans-border access to stored computer data with consent or where publicly available</b></p> <p>A Party may, without the authorisation of another Party:</p> <ul style="list-style-type: none"> <li>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</li> <li>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</li> </ul>	
<p><b>Article 33 – Mutual assistance in the real-time collection of traffic data</b></p> <p>1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p><b>Article 34 – Mutual assistance regarding the interception of content data</b></p> <p>The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.</p>	
<p><b>Article 35 – 24/7 Network</b></p> <p>1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:</p> <ul style="list-style-type: none"> <li>a the provision of technical advice;</li> <li>b the preservation of data pursuant to Articles 29 and 30;</li> <li>c the collection of evidence, the provision of legal information, and locating of suspects.</li> </ul> <p>2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.</p> <p>b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	<p>The Cyber-Police Department of the National Police of Ukraine, as part of the Ministry of Internal Affairs, performs the functions of the 24/7 point of contact under Article 35 of the Convention.</p>
<p><b>Article 42 – Reservations</b></p> <p>By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2,</p>	<p>Reservation contained in the instrument of ratification deposited on 10 March 2006 - Or. Engl.</p> <p>Ukraine reserves the right not to apply paragraph 1 of Article 6 of the Convention concerning the establishment of criminal liability for the production,</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.</p>	<p>procurement for use and otherwise making available for use of the objects designated in subparagraph 1.a.i., and also the production and procurement for use of the objects designated in subparagraph 1.a.ii of Article 6 of the Convention.            Period covered: 01/07/2006 -            Articles concerned : 6</p> <p>Reservation contained in the instrument of ratification deposited on 10 March 2006 - Or. Engl.</p> <p>Ukraine reserves the right not to apply to the full extent subparagraphs 1.d and 1.e of Article 9 of the Convention.            Period covered: 01/07/2006 -            Articles concerned : 9</p> <p>Declaration contained in the instrument of ratification deposited on 10 March 2006 - Or. angl.</p> <p>In accordance with Article 24, subparagraph 7.a, of the Convention, Ukraine declares that the authorities empowered to perform the functions mentioned in paragraph 7 of Article 24 of the Convention shall be the Ministry of Justice of Ukraine (concerning court's inquiries) and the General Prosecutor's Office of Ukraine (concerning inquiries of bodies of prejudicial inquiry).            Period covered: 01/07/2006 -            Articles concerned : 24</p> <p>Declaration contained in the instrument of ratification deposited on 10 March 2006 - Or. angl.</p> <p>In accordance with Article 27, subparagraph 2.c, of the Convention, Ukraine declares that the authorities responsible for sending requests for mutual assistance, answering them, their execution or their transfer to the empowered authorities shall be the Ministry of Justice of Ukraine (concerning courts' commission) and the General Prosecutor's Office of Ukraine (concerning commissions of bodies of prejudicial inquiry).            Period covered: 01/07/2006 -            Articles concerned : 27</p>



