Strasbourg, 24 October 2016 **CDL-REF(2016)058**

**Opinion No. 859 / 2016** Or.Engl.

**EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW**
**(VENICE COMMISSION)**

# REPUBLIC OF MOLDOVA

# DRAFT LAWS
# (n°161 and n°281)

# AMENDING AND COMPLETING

# EXISTING LEGISLATION
# ON THE SO-CALLED "MANDATE OF SECURITY"

## (and Explanatory Table to Draft Law n°161)

***Draft***
**n° 161**

**PARLIAMENT OF THE REPUBLIC OF MOLDOVA**

**L A W**
**regarding the amendment and completion of certain legislative acts**

Parliament adopts this organic law.

**Article I.** – In article 7 letter e) of Law no. 753-XIV of 23 December 1999 regarding the Security and Intelligence Service of the Republic of Moldova (Official Gazette of the Republic of Moldova, 1999, no. 156, article 764), subsequently amended and completed, after the phrase „the technical support of the interception of" the phrase „computer data and of" shall be added.

**Article II.** – The Criminal Code of the Republic of Moldova no. 985-XV of 18 April 2002 (republished in the Official Gazette of the Republic of Moldova, 2009, no. 72-74, article 195), subsequently amended and completed, shall be amended and completed as follows:

1. Throughout the Code, the word „telecommunications", in any grammatical case, shall be replaced by the phrase „electronic communications systems", in the respective grammatical case.

2. In article 178 paragraph (1), the phrase „telegraphic notices" shall be replaced by the phrase „electronic communications".

3. Article $208^1$:
In the provision, after the word „the use" the phrase „ , the deliberate obtaining, by means of information technologies or electronic communications systems, of access to" shall be added;
In the sanction, the phrase „from 1 to 3 years" shall be replaced by the phrase „from 3 to 7 years".

4. Article 259:
In paragraph (1), the phrase „and has caused large-scale damages" shall be excluded;
In paragraph (2), letter h) shall have the following content:
,,h) causing large-scale damages".

5. In the sanction of article 260, the phrase „from 500 to 1000 conventional units" shall be replaced by the phrase „from 200 to 500 conventional units", and the phrase „from 2 to 5 years" shall be replaced with the phrase „of up to 3 years".

6. In the sanction of article $260^1$, the phrase „from 2 to 5 years" shall be replaced by the phrase „of up to 5 years".

7. Article $260^2$:
In the provision, after the word „intentional" the word „unauthorised" shall be inserted, and the phrase „ , if these actions have caused large-scale damages," shall be excluded;
In the sanction, the phrase „from 2 to 5 years" shall be replaced by the phrase „of up to 5 years".

8. Article 260[3]:

paragraph (1):

In the provision, after the word „deteriorating" the phrase „ ,in an intentional and unauthorised manner, " shall be added, and the phrase „ , if these actions have caused large-scale damages," shall be excluded;

In the sanction, the phrase „from 2 to 5 years" shall be replaced by the phrase „of up to 5 years";

Paragraph (2), letter d) shall have the following content:

„d) that has led to large-scale damages".

9. Article 260[4]:

Paragraph (1):

In the provision, the phrase „ , if these actions have caused large-scale damages," shall be excluded;

In the sanction, the phrase „from 2 to 5 years" shall be replaced by the phrase „of up to 3 years";

In paragraph (2), letter d) shall have the following content:

„d) that have led to large-scale damages".

10. In the sanction of article 260[5], the phrase „ from 2 to 5 years" shall be replaced by the phrase „of up to 5 years".

11. Article 260[6]:

Paragraph (1):

In the provision, before the word „insertion", the phrase „intentional and unauthorised" shall be introduced, and the phrase „ if these actions have caused large-scale damages," shall be excluded;

In the sanction, the phrase „from 2 to 5 years" shall be replaced with the phrase „of up to 5 years";

Paragraph (2):

In the provision, letter b) shall have the following content:

,,b) that have led to large-scale damages ";

In the sanction, the phrase „from 4 to 9 years" shall be replaced with the phrase „from 4 to 10 years";

shall be completed with paragraph (3) as follows:

„ (3) The actions provided for in paragraph (1) or (2) of this article, that have led to especially large-scale damages,

shall be punished with a jail term from 8 to 15 years."

12. Article 261[1]:

Paragraph (1):

In the provision, phrase „ , if this has led to large-scale damages," shall be excluded;

In the sanction, the phrase „of up to 1 year" shall be replaced with the phrase „of up to 2 years";

Paragraph (2):

In the provision, letter e) shall have the following content:

„e) that has led to large-scale damages".

**Article III.** – The Code of Criminal Procedure of the Republic of Moldova no. 122-XV of 14 March 2003 (republished in the Official Gazette of the Republic of Moldova, 2013, no. 248-251, article 699), subsequently amended and completed, shall be amended and completed as follows:

1. The Code shall be completed with article 130[1] having the following content:

„Article 130[1]. Computer data search and seizure of objects containing computer data

(1) Computer search means the process of looking for, researching, discovering, identifying and accumulating computer data existing in a computer system or computer data storage medium that are relevant for the criminal case, carried out through technical methods and means that ensure the integrity and authenticity of the information contained thereon.

(2) Computer search shall be carried out following a reasoned ordinance of the criminal investigation body and only upon authorisation by the investigating magistrate.

(3) While carrying out the computer search and/or seizure of objects containing computer data, the presence of the person subject to the search and/or seizure or of adult members of their family or of those who represent their interests must be guaranteed. If the presence of these persons is not possible, the representative of the executorial authority of the local public administration shall be invited.

(4) The computer search and the seizure of objects containing computer data at the premises of state institutions, enterprises, organisations and military units shall be carried out in the presence of this representative.

(5) In the case in which, during the search of a computer system or of a computer data storage medium, it is established that the searched computer data are partially or entirely contained in another computer system or computer data storage medium and are legally accessible from the system or medium initially searched or are available for the system or medium initially searched, the search of the other computer system or data storage medium may be carried out following a reasoned ordinance of the prosecutor, without the authorisation of the investigating magistrate, under the obligation to submit immediately to the latter, no later than 24 hours from the conclusion of the computer search, the computer data obtained in result, indicating the reasons for its carrying out. The investigating magistrate checks the legality of this procedural action.

(6) In the case of establishing that the computer search carried out under the terms of article (5) of this article has been legally conducted, the investigating magistrate shall confirm its results in a reasoned conclusion. Otherwise, in a well-founded ruling, they shall acknowledge the search of the other computer system or storage medium to be illegal.

(7) In the case in which, the seizure of the objects containing computer data may seriously affect the authorised provision of public electronic communication networks and services, the criminal investigation body shall order through a reasoned ordinance, the copying of these computer data. In other cases, in which the respective objects are not used for the authorised provision of public electronic communication networks and services, but their seizure might seriously affect the activity of the person who owns or controls them, the criminal investigation body may order, through a well-founded ordinance, the copying of these computer data. The given copies shall serve as means of evidence and shall be made using technical means and methods that ensure the integrity and authenticity of computer data.

(8) In the case in which, the carrying out of the computer search requires a long term, the person in charge of the criminal investigation shall seize the objects containing computer data in order to examine them at the premises of the criminal investigation body. For this purpose, the objects containing computer data shall be packed and sealed and the package shall be signed and the corresponding mention shall be introduced in the minutes.

(9) In addition to the provisions of article 260, the minutes regarding the computer search must comprise information on:

a) the description and listing of computer systems or computer data storage media subject to the search;

b) the description and listing of the activities carried out;

c) the description and listing of computer data discovered during the computer search.

(10) the computer search and the seizure of the objects containing computer data shall be carried out in accordance with the provisions of this Code."

2. The articles shall be completed as follows: $132^6$ – with paragraph (6), $132^7$ and $134^3$ – with paragraph (3), 133 – with paragraph (7), $134^5$ – with paragraph (5), $134^4$, $134^6$

and 138[3] – paragraph (2), 136 – paragraph (9), and in article 138[1], paragraph (5) shall be amended, all paragraphs having the following contents:

„The special investigation measure provided for by this article may be ruled in the case provided for in article 132[1] paragraph (2) point. 2) of this code or of an offence provided for in articles 174-175[1], 185[1]-185[3], 208[1], 208[2], 237 and 259-261[1] of the Criminal Code."

3. Article 138[2] shall be completed with paragraph (7) having the following content:

„The special investigation measure provided for in this article may be ruled in the case of offences provided for in article 132[1] paragraph (2) point 2) of this code or of an offence provided for in articles 175[1], 185[1]-185[2], 208[1], 208[2], 237, 260-260[2], 260[4], 260[6] and 261[1] of the Criminal Code."

4. Article 132[2] paragraph (1) point 1):

Shall be completed with letter c[1]) having the following content:

„c[1]) interception and recording of computer data";

In letter d), after the phrase „mail" the phrase "and electronic communications" shall be inserted.

5. In article 132[8] paragraph (2), after the phrase „article 172 paragraphs (2) and (3)" the phrase „ , article 174," shall be added.

6. Article 132[11] shall have the following content:

„Article 132[11]. Interception and recording of computer data

(1)The interception and recording of computer data consists in the use of technical methods and/or means through which are collected in real time the data referring to the cyber traffic and/or data related to contents, associated to the given communications, other than those provided for in article 132[8], transmitted through a computer system, and the storage of information obtained following interception on a technical medium.

(2) The interception and recording of computer data shall be ordered and carried out under the conditions stated in article 132[9], which shall be correspondingly enforced.

(3) The special investigation measure provided for by this article may be ordered in the case of the offences provided for in article 132[1] paragraph (2) point 2) of this code or of an offence provided for in articles 175-175[1], 185[1]-185[3], 208[1], 208[2], 237 and 259-261[1] of the Criminal Code."

7. The law shall be completed with article 132[12] having the following content:

„Article 132[12]. Check of the interception recordings

Evidence means obtained under the conditions of articles 132[8]-132[11] may be checked through technical expertise, ruled by a court on the request of the parties or ex officio."

8. Article 133:

In the title, after the phrase „of mail" the phrase „and of electronic communications" shall be added;

In paragraph (1), after the phrase „mail" the phrase „and/or electronic communications" shall be inserted;

In paragraph (2), after the phrase „mail" the phrase „and/or electronic communications" shall be added, and after the word „fax" the phrase „ , text messaging through computer systems other than telephony services" shall be added;

In paragraph (3), after the phrase „mail" the phrase „and/or electronic communications" shall be added, after the phrase „of the postal institution" the phrase „or, as appropriate, of the provider of email or text messaging services" shall be added and after the phrase „mail" the phrase „and/or electronic communications" shall be added;

In paragraph (4), after the phrase „of the postal institution" the phrase „or, as appropriate, of the provider of email or text messaging services" shall be inserted;

In paragraph (5), after the phrase „of the postal institution" the phrase „or, as appropriate, of the provider of email or text messaging services" shall be inserted;

In paragraph (6), after the phrase „of mail" the phrase „and/or of electronic communications" shall be inserted.

9. Article 134 shall be completed with paragraph (4) having the following content:

„ (4) The provisions of paragraphs (1)-(3) of this article shall be enforced correspondingly in the case of information related to electronic communications, too."

10. Article $134^2$ paragraph (2):
after number „$165^1$" the phrase „ , $175^1$, $185^1$-$185^2$" shall be inserted;
number „208" shall be replaced by the phrase „208-$208^2$";
after number „256" the phrase „, 259-$261^1$" shall be inserted.

11. In article $134^5$ paragraph (1), the word „telecommunications" shall be replaced by the phrase „electronic communications".

12. In article 305 paragraph (3), after the phrase „upon interception and recording of communications" the phrase „, upon interception and recording of computer data" shall be added.

**Article IV.** – In article 17 of Law no. 264-XVI of 27 October 2005 regarding the practice of the medical profession (Official Gazette of the Republic of Moldova, 2005, no. 172-175, article 839), subsequently modified and completed, paragraph (1) shall be completed with letter $e^1$) having the following content:

„$e^1$) to transmit to the law enforcement bodies any information, they have learnt about in the exercise of their job duties, regarding abuse cases and violence, including sexual ones and those directed towards children".

**Art. V.** – In article 20 of the Law on electronic communications no. 241-XVI of 15 November 2007 (Official Gazette of the Republic of Moldova, 2008, no. 51-54, article 155), subsequently modified and completed, paragraph (3) shall be amended as follows:

In letter a), the word "operative" shall be replaced by the word „special";

In letter b), the word „operative" shall be replaced by the word „special".

**Art. VI.** – Contravention Code of the Republic of Moldova no. 218-XVI of 24 October 2008 (Official Gazette of the Republic of Moldova, 2009, no. 3-6, article 15), subsequently completed and amended, shall be amended and completed as follows:

1. The provision of article 90 shall be completed in the end with the phrase „, or their deliberate accessing in public places".

2. Shall be completed with article $247^1$ having the following content:

„Article $247^1$. The breach of the legislation regarding the prevention and combating of cyber crimes

The breach of the legislation regarding the prevention and combating of cyber crimes by the providers of electronic communications services, regardless of the type of ownership or legal form of organisation, expressed through:

a) failure to fulfil the obligation to keep the record of service users;

b) failure to communicate to the competent authorities the illegal access to the information in the computer system, the attempts to introduce illegal programmes, the violation by responsible persons of the rules for the collection, processing, storage, dissemination and distribution of information or of the rules regarding the protection of the computer system established in agreement with the status of the information or with its degree of protection, if these have contributed to the appropriation, distortion or destruction

of information or have led to other serious repercussions, the disturbance of the functioning of computer systems, other computer security incidents with a significant impact;

c) failure to comply, in confidence, with the request of the competent authority with regard to the rapid preservation of computer data or of the data referring to the information traffic, indicated in the respective request, which are in danger of destruction or alteration, under the conditions established by law;

d) failure to submit to the competent authorities, following a request made under the terms of procedural legislation, of the data referring to information traffic or users;

e) failure to enforce security measures through the employment of certain procedures, devices or specialised software with which the access to the user's own computer system might be restricted or forbidden without such a right;

f) failure to ensure the preservation of data referring to the traffic, under the conditions established by law, in order to identify service providers, service users and the channel through which the communication has been transmitted;

g) failure to fulfil the obligation to stop, using owned technical methods and means, under the conditions established by law, the access to all IP addresses where web pages are located, including those hosted by the respective provider, which contain child pornography, promote sexual abuse or sexual exploitation of children, contain information propagating war or terrorism, incite to national, racial or religious hate or discrimination, to hostility or violence, contain or disseminate instruction concerning the manner of committing crimes,

shall be sanctioned with a fine from 100 to 150 conventional units imposed to natural persons and a fine from 400 to 500 conventional units imposed to legal persons."

3. Article 252 shall be excluded.

4. In article 400 paragraph (1), after the number „245" the text „, $247^{1}$" shall be introduced.

**Article VII.** – Law no. 20-XVI of 3 February 2009 regarding the prevention and combating of cyber crimes (Official Gazette of the Republic of Moldova, 2010, no. 11-12, article 17), subsequently amended and completed, shall be amended and completed as follows:

1. Article 2 shall be completed with the following notions:

*„critical infrastructure* – an element or a system, located on the territory of the state, which is essential for maintaining the functions of ensuring the health, security, social, economic and other kinds of welfare of the population, which disturbance or destruction may have a negative impact, as a result of the incapacity to carry along these functions;

*owner/operator/administrator of the critical infrastructure* – any entity established by Government to be the holder of an element or of a system that is part of the critical infrastructure or is in charge of its operation/administration;

*preservation of data* – the keeping and protection of the integrity of the data existing in a computer system, owned and controlled by a person;

*computer data security* – a state of normality resulted from implementing a set of measures through which confidentiality, integrity, availability and authenticity of computer data and public or private services and resources are guaranteed, including by preventing and combating cyber criminality;

*Computer security incident* – a disruption of computer security that has or may have a negative impact on keeping the confidentiality, integrity, availability and authenticity of electronic information and public or private resources or services;

*Cyber criminality* – negative social phenomena characterised by a set of criminal activities in which computer data and/or computer systems are an instrument for the commission of the crime or an object of the crime."

2. Article 4 shall have the following content:

"Article 4. Responsibilities of law enforcement bodies in preventing and combating cyber criminality.

(1)The framework of the Prosecutor General`s Office, the General Police Inspectorate of the Minister for Internal Affairs and the Security and Intelligence Service shall comprise specialized divisions, whose responsibilities shall include preventing and combating cyber criminality and which shall work together to fulfil the given responsibilities.

(2) The General Police Inspectorate shall carry out the activity of preventing and combating cyber criminality, in accordance with the legislation in force, including through special investigative activity and the conduct of criminal investigation in cyber criminality cases, an order regarding the rapid preservation of computer data or data related to information traffic, the appointment of a contact point responsible for ensuring international cooperation in combating cybercrime, the carrying out of international cooperation, the analysis of the cyber criminality trend and the identification and protection of cyber criminality victims.

(3) The General Police Inspectorate and the Security and Intelligence Service, with the participation of other public authorities and private institutions shall develop, manage and update by means of an automatic information system, databases on the phenomenon of cyber criminality.

(4) The General Police Inspectorate and the Prosecutor General`s Office shall jointly carry out studies aimed at detecting and eliminating the causes and conditions that favour cyber criminality and publish their results through mass media.

(5) The Prosecutor General`s Office:

a) shall carry out, within the limits of its competence, activities of prevention and combating of cyber criminality, in accordance with the current legislation;

b) shall coordinate, lead and conduct the criminal investigation in cyber criminality cases;

c) shall represent in court the accusation on behalf of the state;

d) shall receive and transmit requests for international legal assistance, extradition or provisional detention made at the criminal investigation stage;

e) shall order during the criminal investigation stage, upon request of the criminal investigative body or ex officio, rapid preservation of computer data or data relating to information traffic, which are in danger of destruction or alteration, under the conditions of criminal procedure legislation;

f) shall take other measures aimed at preventing and combating cyber criminality.

(6) The Security and Intelligence Service shall perform activities aimed at preventing and combating cyber criminality that pose threats to national security, including special investigation work, revealing activity of international criminal groups and organisations, other activities within its competence.

(7) The National Institute of Justice shall carry out the personal development of the staff engaged in the administration of justice in the fight against cyber criminality."

3. The law shall be completed with article $4^1$ having the following content:

Article $4^1$. The National Plan for preventing and combating cyber criminality

(1) In order to prevent and combat cyber criminality, as well as to ensure the protection of its victims, the Government shall approve the National Plan for preventing and combating cyber criminality (hereinafter the National Plan), drawn up with consideration of the opinion of the Prosecutor General`s Office.

(2) The National Plan shall be approved periodically, for a three years term and shall provide for the implementation of complex actions, the carrying out of socio-economic initiatives aimed at preventing and combating cyber criminality as well as protecting its victims, including through cooperation with international organisations, nongovernmental organisations, other institutions and representatives of civil society.

(3) Central public administration authorities responsible for preventing and combating cyber criminality, shall adopt their own action plans to implement the National Plan in their own fields of activity.

4. Article 5 shall be completed with paragraph (2) having the following content:

"(2) Service providers, nongovernmental organisations, civil society representatives and other persons shall be encouraged to communicate to the General Police Inspectorate or to the Prosecutor General`s Office any information they have learnt with respect to private or legal persons who share, disseminate, import or export images containing representations of one or more children involved in sexual activities and also with respect to sexual abuse of children committed through electronic communications."

5. The law shall be completed with article $6^1$ having the following content:

Article $6^1$. Obligations of owners and operators of critical computer infrastructures.

In order to prevent cyber criminality, owners and operators of critical computer infrastructures are obliged to:

a) implement the minimum requirements established by the responsible state authority with respect to the security of owned or operated critical computer infrastructures.

b) create a contact point in order to interact with public authorities and state institutions empowered to ensure the security of critical computer infrastructures.

c) cooperate with the competent authorities in ensuring the security of critical computer infrastructures owned or operated.

d) communicate immediately to the competent authorities, no later than 24 hours from the moment of detection, information about the illegal access to their own computer data system, attempts to introduce illegal programmes, the violation by responsible persons of the rules regarding collection, processing, storage, dissemination and distribution of information or of the rules regarding the protection of the computer system established in agreement with the status of the information or with its degree of protection, if these acts have contributed to the appropriation, distortion or destruction of information or have led to other serious repercussions, the disruption of the functioning of computer systems, other computer security incidents with a significant impact."

6. Article 7:

Paragraph (1):

Letter a) shall be completed at the end with the phrase: "and in case of prepaid anonymous services – date and time of the first activation of service";

In letter b), the phrase "data about information traffic, inclusively" shall be substituted with the phrase: ", provided by article 4, paragraph (1),", and the words "information delicts" shall be replaced by the words "information security incidents with significant impact";

In letter c), the word "immediate" shall be replaced by the word "rapid", after the words "information traffic" the text shall be introduced, as follows: ", indicated in the respective request", and the phrase "120 calendar days" shall be replaced by the phrase "180 calendar days";

In letter d), the words "of the law" shall be replaced by "procedural legislation", and after the word "relating" the words "to information traffic and" shall be introduced;

In letter e), the word "a" shall be replaced by the words "its own", and the word "unauthorised" shall be replaced by the words "without such a right";

In letter f), the text "monitoring, surveillance and" shall be excluded, and the phrase "for a period of 180 calendar days" shall be replaced by the phrase "in fixed and mobile telephony network for a period of one year, and of those relating to Internet traffic and Internet telephony – for a period of 6 months";

In letter g), after the word "network" the text "based on the request of the competent authority referred to in article 4, paragraph (1), within the limits of its technical performances,";

Letter h) shall be added, with the following content:

h) to stop, under the provisions of the law, from own computer system, using available technical methods and means, the access to all IP addresses on which web pages are located, including those hosted by the concerned provider, which contain child pornography, promote sexual abuse or child sexual exploitation, contain information which propagates war or terrorism, urges to hatred and national, racial or religious discrimination, to hostility or violence, contain or disseminate instructions on how to commit crimes",

In the paragraph (2), the word "immediately" shall be replaced by the words "in reasonable terms".

7. Article 10:

In paragraphs (1) and (2), the word "immediate" shall be replaced by the word "rapid";

Paragraph (5) shall be added, as follows:

"(5) If the competent authority from the Republic of Moldova finds out that a service provider, had, while executing a request of traffic-related data preservation, participated in the transmission of this communication in another state, it shall rapidly disclose to the requesting foreign competent authority an adequate amount of traffic-related data, in order to identify the service provider and the channel the information was transmitted thereby."

**Art. VIII.** – Article 18 para. (1) point 1) from Law no. 59 of 29 March 2012 on the special investigation activity (Official Gazette of the Republic of Moldova, 2012, nos. 113-118, art. 373), with further amendments and completions, shall be completed as follows:

Letter $c^1$ shall be added, as follows:

„$c^1$) interception and recording of information data";

In letter d), after the words "of mails", the phrase "and/or electronic communications" shall be added.

**Chairman of Parliament**

***Draft***
***no. 281***

**L A W**
**on amendments and supplements to certain legislative acts**

The Parliament adopts this organic law.

**Article I.** – Law no. 837-XIII of 17 May 1996 on public associations (republished in the Official Gazette of the Republic of Moldova, 2007, no.153-156 BIS), with further amendments, shall be supplemented, as follows:

1. Article 4, para (2) shall be supplemented at the end with the text ", as well as of public associations aimed at conducting extremist activity".

*[**Article 4.** Restrictions on the establishment and activity of ublic associations*

*(2) The establishment of paramilitary public associations and of armed formations shall be prohibited.]*

2. Article 36, para. (4) shall be supplemented with letter e¹), as follows:

"e¹) conducting extremist activity;"

***[Article 36.** Dissolution*

*(4) Public association may be dissolved by court decision in cases of:]*

**Article II.** – Law no. 753-XIV of 23 December 1999 on Security and Intelligence Service of the Republic of Moldova (Official Gazette of the Republic of Moldova, 1999, no.156, Article 764), with further amendments, shall be amended and supplemented, as follows:

1. Throughout the contents of the law, the word "operative" shall be replaced by the word "special".

2. In Article 7, letter a) introductory part, the syntagm "system of measures" shall be followed by the text ", including of those provided by Law no.59 of 29 March 2012 on special investigation activity,".

*[**Article 7.** Functions of the Service*

*The Service shall have the following functions:*
*a) development and implementation, within its competence, of a system of measures aimed at the detection, prevention and counteracting of the actions, which endanger, according to the law, the state security, public and human security:]*

3. After Article 7, new Article 7¹ and Article 7² shall be inserted, as follows:

"Article 7¹. Security warrant

(1) In order to carry out its duties, to collect information on possible events and/or actions that may jeopardize the state security, the Service can carry out, outside of criminal

proceedings and based on a security warrant, the measures provided for in Article 18, para. (1) p. 1) of Law no. 59 of 29 March 2012 on special investigation activity.

(2) In compliance with the provision of Article 22 para. (5) letter h) of the Law on financial institutions no. 550-XIII of 21 July 1995, by derogation from the provisions of para. (1) of this Article, the special investigation measure provided for in Article 18 para. (1) p. 1) letter f) of Law no. 59 of 29 March 2012 on special investigation activity shall be carried out outside of criminal proceedings, without security warrant only to the extent that it relates to the access to financial information.

(3) The security warrant shall be issued following a justified order of a specially appointed judge within the Chisinau Court of Appeal, according to the justified approach of the prosecutor, issued on the grounds of the proposal of the investigation officer of the Service.

(4) The persons appointed as the judge mandated to consider the approach as indicated under para. (3) and, respectively, as the prosecutor empowered to issue this approach, shall be entitled to state secrecy access under Law no. 245-XVI of 27 November 2008 on state secrets.

(5) The examination of the approach on the issue of security warrant shall be conducted no later than four hours after the submission thereof, in closed session, with the participation of the prosecutor and the investigation officer. In the event that the approach is declined, no repeated approach on the same grounds and on the same persons shall be admitted.

(6) The approach on the issue of security warrant shall contain the following data:

a) name, surname and position of the person requesting the warrant issue;
b) personal identification data of the person subject to special investigation measure, if these are known;
c) special investigation measure for which the authorisation is requested;
d) factual circumstances serving as ground for conducting the special investigation measure and, where necessary, possible consequences thereof;
e) results expected to be obtained following the special investigation measure;
f) the term of conducting the respective measure;
g) the location of conducting the special investigation measure;
h) other data that are important to justify the special investigation measure, which would ensure the legal and justified authorisation thereof.

The materials confirming the need for a special investigation measure shall be attached to the approach on the issue of security warrant.

(7) The order of the judge on the issue of security warrant shall contain the following data: date and place of the order writing; name and surname of the judge; name and position of the person requesting the warrant; the body conducting the special investigation measure; identification data of the person subject to special investigation measure, if these are known; data justifying the need for conducting and, respectively, authorising the special investigation measure; authorised special investigation measures; time limits for conducting the special investigation measure; the location of conducting the special investigation measure; other data that are

important to justify the authorisation of the special investigation measure.

(8) The security warrant can be issued in relation to:

a) a person, both identified and unidentified, on whom information exists that he/she is preparing, is undertaking attempts to commit or has committed one or more deeds indicated in Art. 7 letter a) or d) of this law or in Art. 4 para. (2) of the Law on state security no. 618-XIII of 31 October 1995;

b) a person, both identified and unidentified, on whom information exists that he/she is receiving or is sending information or goods from/to persons mentioned under letter a) of this paragraph or are intended for these persons;

c) a person, both identified and unidentified, other than those mentioned under letter a) and letter b) of this paragraph, if there is information that the communication devices, the domicile or the goods of this person are used by persons mentioned under letter a) and/or letter b) of this paragraph for the purposes mentioned under letter a);

d) a person, both identified and unidentified, other than those mentioned under letters a)–c) of this paragraph, if his/her monitoring may lead to the disclosure of the location of persons referred to under letter a) and/or letter b) of this paragraph or of their full identity.

(9) The maximum period that may be authorised for conducting special investigation measures under a security warrant, is 30 days. If necessary, this period may be extended for periods of up to 30 days, and the total cumulative duration of conducting a special investigation measure on a person for a concrete deed, shall not exceed two years. The judge shall be required, upon each request of period extension for conducting the special investigation measure, to consider the circumstances, which justify this extension, and if it is deemed that the request is not justified, shall deny the extension.

(10) The order of the judge on the denial of the issue of security warrant or on the denial to extend the deadline for conducting the special investigation measure can be appealed in the Supreme Court within 5 working days. The appeal shall be examined in closed session by a special judge appointed by the Chairman of the Supreme Court, who is entitled to state secrecy, under Law no. 245-XVI of 27 November 2008 on state secrets.

(11) As an exception, special investigation measures that are to be carried out under a security warrant can be conducted without a security warrant, based on a justified writ of the prosecutor, when there are exceptional circumstances not allowing postponement and the security warrant cannot be obtained without an essential risk of delay, which fact can result in relevant information loss or jeopardize the security of persons. In this case, the judge shall be informed within 24 hours from ordering the measure on the performance thereof, and shall be submitted all materials with arguments in favour of the need to conduct the special investigation measure, as well as the circumstances not allowing the postponement thereof. If there are sufficient grounds, the judge shall confirm, through a justified order, the lawfulness of conducting the measure. Otherwise, the judge shall declare the illegality of carrying out the measure, and shall order its suspension and destruction of the material information carrier and of materials collected during the conduct of special investigation measure. The order of the judge may be appealed under para. (10). The appeal shall suspend the destruction of the material information carrier and of collected materials.

(12) The approach for the security warrant request, the court order on security warrant, as well as other materials from the file on security warrant shall be state secret.

Article $7^2$. Notification of the person about the actions carried out in his/her regard under security warrant

(1) After the dismissal of the special file on conducting special investigation measures authorised under a security warrant, the Service shall, within 5 working days following the date of dismissal, notify the person against whom such actions have been carried out. Materials confirming the notification of the person shall be attached to the special file.

(2) In each case of notification of the person in respect of whom special investigation measures authorised under a security warrant have been carried out, the Service shall notify the judge who issued the security warrant and the prosecutor who participated in the authorization of such measures.

(3) The notification shall not be done if there are reasonable grounds to consider that this could pose an increased risk to human life or health, jeopardize another ongoing investigation, damage state security or harm the purpose for which the special investigation measures have been carried out.

(4) The investigation officer who manages the special file shall write a report on the existence of the grounds mentioned under para. (3), where these grounds are featured in detail, and shall submit it for approval to the Director of the Service. If the report is approved, the investigation officer shall notify accordingly the prosecutor who participated in authorising special investigation measures, while the latter shall request from the judge, who issued the security warrant, the authorisation to refrain from notifying the person. The denial to authorise the refraining from notification can be challenged by the prosecutor, applying the provisions of Art. $7^1$ para. (10).

(5) The order of the judge on the authorisation to refrain from notification, as well as the approved report shall be attached to the special file."

**Art. III.** – The Criminal Code of the Republic of Moldova no. 985-XV of 18 April 2002 (republished in the Official Gazette of the Republic of Moldova, 2009, no. 72–74, Art. 195), with further amendments, shall be amended and supplemented as follows:

1. After Article $134^{13}$, Articles $134^{14}$ and $134^{15}$ shall be inserted with the following contents:

"Article $134^{14}$. Extremist organisation and extremist materials

(1) Extremist organisation means a registered or unregistered organisation or legal entity, in respect of which there is a final court decision on cessation or suspension of activity related to the conduct of extremist activity, issued under Law no. 54-XV of 21 February 2003 on counteracting extremist activity, and which is included in the Register of extremist organisations and extremist materials.

(2) Extremist material means the information or the document, including of anonymous nature, on any medium, on which there is a final court decision regarding the declaring of the material as of extremist nature, issued under Law no. 54-XV of 21 February 2003 on counteracting extremist activity, which is included in the Register of extremist organisations and extremist materials.

Article $134^{15}$. Unconstitutional entity

Unconstitutional entity means the structure created outside the constitutional and legal regulations of a state, on a territory, not recognized by that state and by most countries of the world."

2. After Article 337, Article $337^1$ shall be inserted with the following contents:

"Article $337^1$. Serious endangerment of the security of the Republic of Moldova

(1) Serious endangerment of the security of the Republic of Moldova, i.e. the act committed intentionally by a citizen of the Republic of Moldova, a foreign citizen or a stateless person to the detriment of sovereignty, independence, territorial inviolability, state security or defence capacity of the Republic of Moldova manifested by one of the following actions:

a) transfer, theft or collection of information constituting a state secret in order to deliver it to the representatives of an unconstitutional entity, of an organisation or to agents thereof;

b) transfer, theft or collection of information other than that mentioned under letter a) by order of the intelligence service of an unconstitutional entity for the purpose of using it to the detriment of the interests of the Republic of Moldova;

c) assisting the administration of an unconstitutional entity in conducting hostile activities against the Republic of Moldova,

shall be punished by imprisonment from 12 to 20 years.

(2) The person recruited by the intelligence service of an unconstitutional entity that has not committed any action for achieving the assigned tasks and declared voluntarily to the authorities his/her connection with the intelligence service of the unconstitutional entity shall be exempted from criminal liability for carrying out one of the acts mentioned under para. (1)."

3. After Article 340, Article $340^1$ shall be inserted with the following contents:

"Article $340^1$. Illegal actions threatening the constitutional regime, the independence, the integrity or the territorial inviolability of the Republic of Moldova

(1) Actions aimed at changing the constitutional regime of the Republic of Moldova, at undermining, suppressing or eliminating sovereignty, independence, territorial integrity or inviolability thereof contrary to the provisions of the Constitution of the Republic of Moldova shall be punished by a fine in an amount of 500 to 1000 conventional units or by imprisonment of up to 6 years.

(2) The same acts:

a) committed by two or more persons;

b) committed by a public person, by an official, a dignitary, a foreign public person or an international official;

c) accompanied by death threats or bodily injury or damage to health;

d) accompanied by violence unharmful to life or health;

e) accompanied by destruction of property

shall be punished by imprisonment from 3 to 8 years with the deprivation of the right to hold certain positions or engage in certain activities for up to 5 years.

(3) Acts provided for under para. (1) or (2):

a) committed by an organised criminal group, a criminal organisation or extremist organisation;

b) resulting in large damages;

c) accompanied by violence harmful to life or health;
d) committed by using weapons;
e) committed at the request of a foreign state, a foreign organisation, an unconstitutional establishment or of the representatives thereof, shall be punished by imprisonment from 7 to 15 years.

(4) Acts provided for under para. (1), (2) or (3), which caused the death of one or more persons, shall be punished by imprisonment from 12 to 18 years."

4. Article 341 shall have the following contents:

"Article 341. Appeals threatening the constitutional regime of the Republic of Moldova

(1) Public appeals or dissemination, through various ways, of appeals aimed at:
a) overthrowing or changing, through violence or other illegal actions, of the constitutional regime;
b) violation of the territorial integrity of the Republic of Moldova
shall be punished by imprisonment from 1 to 3 years.

(2) The same acts committed by two or more persons
shall be punished by imprisonment from 2 to 4 years.

(3) Actions provided under para. (1) or (2), committed at the request of a foreign state, foreign organisation, unconstitutional establishment or of certain representatives thereof, shall be punished by imprisonment from 3 to 7 years."

5. After Article 346, Articles $346^1$–$346^3$ shall be inserted, as follows:

"Article $346^1$. Creation, management or organisation of activity of an extremist organisation or participation thereto

(1) Joining the membership of an extremist organisation or contributing in every way to the activity of such an organisation shall be punished by a fine in an amount from 200 to 700 conventional units or by imprisonment of up to 3 years, in both cases with (or without) the deprivation of the right to hold certain positions or conduct certain activities for up to 2 years, and the legal entity shall be punished by a fine in an amount from 3000 to 5000 conventional units with the liquidation thereof.

(2) Creation in full awareness of an organisation with the purpose of conducting extremist activities, management or establishment of the activity of an extremist organisation shall be punished by a fine in an amount from 600 to 1000 conventional units or by imprisonment of up to 5 years, in both cases with the deprivation of the right to hold certain positions or conduct certain activities for a term of 2 to 5 years, and the legal entity shall be punished by a fine in an amount from 3000 to 7000 conventional units with the liquidation thereof.

Article $346^2$. Dissemination and use of materials of extremist nature

(1) Introduction on the territory of the Republic of Moldova of materials of extremist nature for dissemination purposes, offering for sale, selling, dissemination in any other way, as well as production or possession for dissemination purposes of such materials shall be punished by a fine in an amount from 200 to 500 conventional units or

by unpaid community work from 140 to 200 hours, or by imprisonment of up to 6 months, and the legal entity shall be punished by a fine in an amount from 3000 to 5000 conventional units with the liquidation thereof.

(2) Use of extremist materials in public with the purpose of urging the pursuit of extremist activities shall be punished by a fine in an amount from 200 to 700 conventional units or by unpaid community work from 180 to 240 hours, or by imprisonment of up to 1 year, and the legal entity shall be punished by a fine in an amount of 7000 conventional units with the liquidation thereof.

(3) Acts provided for under paras. (1) or (2) committed for either educational, scientific, artistic, collection purposes or in order to provide information on historical or current events shall not be deemed as offences.

Article $346^3$. Propagation of the Nazi, racist or xenophobic ideology, of symbols thereof

(1) Introduction on the territory of the Republic of Moldova, for dissemination purposes, of Nazi, racist or xenophobic attributes or symbols, of certain similar attributes or symbols, leading to confusion with Nazi, racist or xenophobic attributes or symbols, offering for sale, selling, dissemination in any other way, as well as production or possession for dissemination purposes of such attributes or symbols shall be punished by a fine in an amount from 200 to 500 conventional units or by unpaid community work from 140 to 200 hours, or by imprisonment for a term of up to 6 months, and the legal entity shall be punished by a fine in an amount from 3000 to 5000 conventional units with the liquidation thereof.

(2) Propagation of Nazi, racist or xenophobic ideology by any means shall be punished by a fine in an amount of up to 250 conventional units or by imprisonment for a term of up to 3 years, in both cases with the deprivation of the right to hold certain positions or conduct certain activities from 2 to 5 years, and the legal entity shall be punished by a fine in an amount from 3000 to 7000 conventional units with the liquidation thereof.

(3) Acts provided for under para. (1) committed for either educational, scientific, artistic, collection purposes or in order to provide information on historical or current events shall not be deemed as offences."

**Art. IV.** – Law no. 54-XV of 21 February 2003 on counteracting extremist activity (Official Gazette of the Republic of Moldova, 2003, no. 56–58, Art. 245) shall be amended and supplemented as follows:

1. Article 1:

***[Article 1.*** *Main notions*
*By virtue of this law, the notions below shall have the meaning as follows:*

*a) the activity of the public or religious association, of mass medium, of another organization or of a physical person with the purpose of planning, organising, preparing or carrying out certain actions aimed at:]*

Under notion “extremist activity”: letter a): in the introductory part, the words “of the public or religious association” shall be replaced by the text “of the public association, religious cult or of a component part thereof”, and after the words “of mass media or of another”, the words “registered or unregistered” shall be added (hereinafter – *other organisation*)”;

at the end, three new hyphens shall be added, as follows:

“ -desecration of national state symbols (flag, coat of arms, anthem) of the Republic of Moldova or of another state, hoisted, used or sung publicly, for the purposes of changing through violence the base of the constitutional system, of violating the integrity of the Republic of Moldova, of usurping the state power or the official quality, of humiliating the national dignity;

- propagation of the Nazi, racist or xenophobic ideology;
- infringement, through violence, of rights, freedoms or legitimate interests of persons based on race, colour, nationality, ethnic origin, language, religion or belief, sex, age, disability, opinion, political affiliation or any other criterion;”

Letter b) shall have the following contents:

“b) introduction on the territory of the Republic of Moldova, for dissemination purposes, offering for sale, selling, dissemination in any other way, production for dissemination purposes, propagation or public display of:

- Nazi attributes or symbols, of similar attributes or symbols, leading to confusion with Nazi attributes or symbols;
- other attributes or symbols with racist or xenophobic meaning;”

The notion “extremist organisation” shall have the following contents:

“*extremist organisation* – registered or unregistered organisation or legal entity, on which there is a final court decision on cessation or suspension of activity related to the conduct of extremist activity, issued under this law, and which is included in the Register of extremist organisations and extremist materials;”.

2. In Article 2 letter f), the text “public and religious associations” shall be replaced by the text “public associations, religious cults or component parts thereof”.

***[Article 2.*** *Basic principles of counteracting extremist activity*

*Counteracting of extremist activity shall be based on the following principles:*

*f) collaboration of the state with public and religious associations, mass media, with other organisations and natural persons for counteracting extremist activity;]*

3. In Article 3 letter b), the text “of public and religious associations” shall be replaced by the text “of public associations, religious cults or component parts thereof”.

***[Article 3.*** *Main directions in counteracting extremist activity*

*Counteracting of extremist activity shall be performed on main directions, as follows:*

*b) detection, prevention and suppression of extremist activity of public and religious associations, of mass media, other organisations and of natural persons*.]

4. Article 4 shall have the following wording:

“Article 4. Entities responsible for counteracting extremist activity

(1) The Security and Intelligence Service is the specialised state body which, through acts of intelligence, counterintelligence and crime control, shall prevent, detect and break extremist activity.

(2) The General Prosecutor’s Office shall counteract extremist activity by managing and conducting criminal investigations.

(3) Central and local public authorities shall participate, within their competence, in the counteracting of extremist activities.

(4) The Security and Intelligence Service may use, jointly with the Ministry of Internal Affairs, Ministry of Defence, the State Protection and Guard Service, and the Customs Service, forces and means thereof for actions of extremist activities counteracting, according to the law.”

5. Article 6 shall have the following contents:

“Article 6. Responsibility of public associations, religious cults or component parts thereof, and of other for conducting extremist activity

(1) The establishment and activity of public associations, religious cults or component parts thereof, of other organisations whose aim or actions involve extremist activity shall be prohibited in the Republic of Moldova.

(2) In case of detection of actions denoting extremism in the activity of a public association, a religious cult or other organisation, including in the activity of at least one territorial branch or other branch thereof, it shall be notified / warned in writing on the inadmissibility of conducting such activities, indicating concrete reasons for the notification / warning, including breaches committed. Where it is possible to take measures to remedy the committed violations, the notification / warning shall also indicate the deadline for their removal, which shall be set as one month from the date of notification / warning.

(3) The notification /warning of the public association, religious cult or a component part thereof or of another organisation shall be made by the Prosecutor General, subordinated prosecutors, the Ministry of Justice or the Security and Intelligence Service.

(4) The notification /warning may be challenged, as per established procedures, in the court.

(5) If the notification / warning has not been challenged in court as per established procedures or have not been declared illegal by the court, as well as if, by the deadline, the respective public association, religious cult, other organisation or the territorial branch, or another branch thereof has not removed the irregularities that served as grounds for notification / warning or if, in the course of 12 months from the date of notification / warning, new actions denoting the existence of signs of

extremism were detected, the court shall issue a decision on the cessation or suspension, for a term of up to one year, of the activity of the respective association, religious cult, the component part thereof or of another organisation, upon the request of the Prosecutor General, subordinated prosecutors, the Ministry of Justice or of the Security and Intelligence Service.

(6) On the grounds of the final court decision regarding the cessation or suspension of activity in connection with extremist activities carrying out, public associations, religious cults, the component parts thereof or other organisations shall be entered in the Register of extremist organisations and extremist materials.

(7) If the court issued, in compliance with this law, the decision on cessation or suspension of activity of the public association, religious cult or another organisation, the activity of territorial branches or other branches thereof shall also be ceased or suspended."

6. Article 7:

***[Article 7.*** *Responsibility of mass medium for dissemination of extremist materials and pursuit of extremist activity]*

in para. (2), the words "that registered this mass medium" shall be followed by the text ", the Security and Intelligence Service";

*[(2) In the event that a mass medium disseminates extremist materials, or actions denoting extremism are detected in the activity thereof, the empowered state authority that registered this mass medium, the General Prosecutor or the subordinated prosecutors shall notify/warn in writing the founder and/or the editorship/editor-in-chief of this mass medium on the inadmissibility of such actions or such activities, revealing the concrete reasons for the notification / warning, including violations committed. If it is possible to take measures to remove the committed violations, the deadline for the removal thereof shall be indicated therein, and it shall be up to one month from the date of the notification/warning.]*

in para. (4), the words "that registered this mass medium" shall be followed by the text " , of the Security and Intelligence Service";

*[(4) If the notification/warning has not been challenged in court, as established, or has not been declared illegal by the court, as well as if, within the established deadline, measures to remove the committed violations that served as grounds for notification / warning have not been undertaken, or if, within 12 months from the date of notification/warning, new actions denoting the existence of signs of extremism in the activity of mass medium have been detected, the court shall pronounce, on the grounds of the request of the empowered state authority that registered this mass medium or of the General Prosecutor or subordinate prosecutors, the decision on the cessation or suspension, for a period of up to one year, of the activity of this mass medium.]*

para. (4) shall be followed by para. ($4^1$), as shown below:

"($4^1$) On the grounds of the final court decision on the cessation or suspension of activity in connection with extremist activities carrying out, the mass medium shall be entered in the Register of extremist organisations and extremist materials."

7. Article 8 shall be worded as follows:

"Article 8. Inadmissibility of the use of electronic communication networks and information systems for carrying out extremist activities

(1) The use of electronic communication networks and of information systems for carrying out extremist activities shall be prohibited.

(2) In the event that the electronic communication networks or the information systems are used to carry out certain extremist activities, the measures stipulated in the enforced laws and normative acts shall apply.

(3) In the event that a material denoting extremism is placed on the information system (webpage, portal, forum, social network, blog, etc.), the Security and Intelligence Service shall order the network and/or services provider to provisionally deny, on the territory of the Republic of Moldova, the access to this material.

(4) The provisional denial of the access to the material provided in para. (3) shall be ordered for a term of up to 60 days. The Security and Intelligence Service shall be required, within 5 working days after the issue of the order on provisional denial of access to the material denoting extremism, to notify the court for establishing the extremist nature of the material, with a view to undertake, where applicable, other actions stipulated by this law.

(5) The order issued by the Security and Intelligence Service on provisional denial of the access to the material denoting extremism shall be immediately placed on the official webpage of the Security and Intelligence Service, and, at the same time, a written summons shall be addressed to the provider of electronic communication network and/or services regarding its execution.

(6) The provider of electronic communication network and/or services shall be required, within maximum 4 hours from the reception of the summons, to deny the access to the material indicated in the order.

(7) In the event that two or more extremist materials are placed in the information system, the court shall, on the grounds of the request of the Security and Intelligence Service, the General Prosecutor's Office or of the subordinated prosecutors, issue the decision on final or up to one-year denial of the access, on the territory of the Republic of Moldova, to the respective information system or to certain components thereof.

(8) The Security and Intelligence Service shall request the provider of electronic communication network and/or services, to deny, on the grounds of the final court decision, issued under para. (7), the access, on the territory of the Republic of Moldova, to the respective information system. The provider of the electronic communication network and/or services shall be required to comply with the court decision within 24 hours from the reception of the request.

(9) The technical procedure of denying the access to the extremist material or to the information system, ordered according to the provisions of this Article, shall be regulated by the Rules of procedure developed jointly by the Ministry of Information Technology and Communications and the Security and Intelligence Service and approved by the Government."

8. Article 9, paragraph (2) shall be supplemented at the end by the text "or of the Security and Intelligence Service".

***[Article 9.*** *Counteracting the dissemination of extremist materials*

*(2) The extremist nature of materials shall be established by the court, upon the intimation of the prosecutor.]*

9. Article 10 shall be worded as follows:

Article 10. Register of extremist organisations and extremist materials

(1) The Security and Intelligence Service shall keep the Register of extremist organisations and extremist materials.

(2) A copy of the final court decision on the cessation or suspension of the activity of an organisation, a legal entity or on the assertion of the extremist nature of an information material shall be submitted to the Security and Intelligence Service that shall enter, by order, the organisation, legal entity or the material indicated in the court decision, in the Register of extremist organisations and extremist materials.

(3) The Order on entering the extremist organisation or the extremist material in the Register of extremist organisations and extremist materials shall be published in the Official Gazette of the Republic of Moldova and on the official webpage of the Security and Intelligence Service.

(4) Dissemination, through any means, on the territory of the Republic of Moldova, of extremist materials entered in the Register of extremist organisations and extremist materials shall be prohibited.

(5) The activity of extremist organisations entered in the Register of extremist organisations and extremist materials, as well as any participation in the activity thereof shall be prohibited.

(6) Persons guilty of knowingly establishing an organisation in order to carry out extremist activities, of joining or participation in the membership of extremist organisations, of dissemination, production or illegal possession, for the purpose of subsequent dissemination, of extremist materials, shall be subject to criminal liability."

10. Article 12:

***[Article 12.*** *Responsibility of the citizens of the Republic of Moldova, foreign citizens and of stateless persons for conducting extremist activities]*

In para. (1), the word "administrative" shall be replaced by the word "contravention";

*[(1) The citizens of the Republic of Moldova, foreign citizens and stateless persons shall be liable, for conducting extremist activity, under criminal, administrative or civil law, as established by legislation.]*

Para. (3) shall have the following wording:

"(3) In the event that the leader or a member of the governing body of the public association, religious cult, of a component part thereof or of another organisation makes a public statement calling to the conduct of extremist activity, without specifying that it is his/her personal opinion, as well as in the case the court

decision is final with regards to such a person for an offence of extremist nature, the respective public association, religious cult, a component part thereof or another organisation shall be required, as soon as possible, to publicly express disagreement on the statements or actions of this person. In case the respective public association, religious cult, component part thereof or another organisation fails to deliver such a statement, this can be construed as a fact denoting signs of extremism in the activity thereof."

11. In Article 13 para. (1), the text "of Law no. 560-XIII of 21 July 1995 on organising and conducting of meetings" shall be replaced by the text "of Law no. 26-XVI of 22 February 2008 on meetings".

*[**Article 13.** Inadmissibility of conducting extremist activity during meetings*

*(1) Extremist activity shall be prohibited during meetings. The organisers of the meeting shall be responsible for compliance with Law no. 560-XIII of 21 July 1995 on organising and conducting of meetings and with other normative acts on non-allowance of extremist activity and timely suppression thereof.]*

12. In Article 14 para. (1), the text "of public, religious associations" shall be replaced by the text "of public associations, religious cults, of".

***[Article 14.** International cooperation in the field of extremism combating*

*(1) The activity of public and religious associations, of other foreign organisations and subdivisions thereof, the activity of which is recognized as an extremist one according to the acts of international law and to the legislation of the Republic of Moldova, shall be prohibited in the Republic of Moldova.]*

**Art. V.** – The Code of criminal procedure of the Republic of Moldova no. 122-XV of 14 March 2003 (republished in the Official Gazette of the Republic of Moldova, 2013, no. 248–251, Art. 699), with further amendments, shall be amended and supplemented, as follows:

1. In Article $132^8$ para. (2), the text "Art. 337–340" shall be replaced by the text "Art. 337–$340^1$", while the text "342–344," shall be followed by the text "Art. $346^1$ para. (2), Art. $346^3$ para. (2),".

2. In Article $134^2$ para. (2), the text "283, 284" shall be replaced by the text "282–285", and the text "343" shall be replaced by the text "337 – $346^3$."

**Art. VI.** – Law no. 59 of 29 March 2012 on special investigation activity (Official Gazette of the Republic of Moldova, 2012, no. 113–118, Art. 373), with further amendments, shall be amended and supplemented, as follows:

1. Article 18:

*[Article 18. Special investigation measures]*

Para. (3) shall be followed by para. ($3^1$):

"($3^1$) In order to collect information about possible events and / or actions that may jeopardize state security, the Security and Intelligence Service can carry out measures provided for in para. (1) outside of criminal proceedings, under Law no. 753-XIV of 23 December 1999 on the Security and Intelligence Service of the Republic of Moldova and this law."

Para. (5) shall be worded as follows:

"(5) In the process of carrying out special investigation measures, information systems shall be used, as well as video and audio recorders, cameras and video cameras, other technical devices, including special technical devices to covertly obtain secret information."

After para. (5), paras. ($5^1$) – ($5^3$) shall be inserted, as follows:

"($5^1$) The classifier of special technical devices for obtaining secret information within the special investigation activity, as well as the rules of procedure on import, export, design, production and marketing of such devices shall be approved by the Government.

($5^2$) Import, export, design, production and marketing of special technical devices for covertly obtaining secret information shall be done only with the approval and for bodies authorised to carry out special investigation activity, intelligence or counterintelligence activity.

($5^3$) The use of special technical devices for covertly obtaining information by physical persons or legal entities not empowered accordingly by law shall be prohibited."

2. In Article 20, after para. (1), para. ($1^1$) shall be inserted, as follows:

*[Article 20. Procedure of authorising special investigation measures]*

"($1^1$) By derogation from the provisions of para. (1) of this Article, special investigation measures specified in Art. 18 para. (1) p. 1) in cases provided for in Art. 18 para. ($3^1$) shall be authorised under Law no. 753-XIV of 23 December 1999 on the Security and Intelligence Service of the Republic of Moldova."

3. In Article 22:

*[Article 22. Registration of the special investigation measure]*

Para. (6) shall be supplemented at the end by the text ", except for cases when the person notification would harm state security";

*[(6) If the lawfulness of conducting special investigation measure is established by writ, the prosecutor shall notify the persons who have been subject to special investigation measure.]*

Para. (7) shall be supplemented at the end by the text ", except for the information assigned to state secret".

*[(7) Since the notification, provided for under para. (6), the person subject to special investigation measure shall have the right to take notice of the minutes on the performance of special investigation measure and of the prosecutor's writ on the lawfulness of the performed measure.]*

4. Article 29 shall be supplemented at the end by the text “with or without the use of technical devices, other than the special ones, for covertly obtaining information”.

*[Article 29. Visual surveillance*

*Visual surveillance shall represent the disclosure and recording of the person’s actions, of certain real estate, means of transport and other facilities.]*

**Art. VII.** – (1) The Government shall, within three months from this law enforcement, bring its normative acts in line with this law.

(2) The Ministry of Justice shall, within one month from the date of this law enforcement, ensure the transmission of the Register of extremist materials to the Security and Intelligence Service.

(3) Within one month from the enforcement of this law:

a) the Chairpersons of Chisinau Court of Appeal and of Supreme Court of Justice shall each appoint a special judge empowered to issue security warrants and to examine appeals in this regard, as well as an alternate judge to replace the first one in his/her absence (paid holiday, sick leave, business trip, etc.), and shall initiate the procedure of entitling them to access the state secret;

b) the Prosecutor General shall appoint a special prosecutor from the General Prosecutor’s Office and an alternate prosecutor to replace the first one in his/her absence (paid holiday, sick leave, business trip, etc.), who are entitled to access the state secret and to submit approaches to the court and issue authorisation orders for special investigation measures, including in exceptional circumstances when no delay is admitted.

**CHAIRMAN OF THE PARLIAMENT**

**ANNEXE**

***Explanatory table***
***for the examination by the Venice Commission of the***
***Draft Law***
***regarding the amendment and completion of certain legislative acts***
***(No.161 of 13.04.2016)***

| *Current legislative norms* | *Norms included in the Draft Law regarding the amendment and completion of certain legislative acts (No.161 of 13.04.2016)* |
|---|---|
| **Law no. 753-XIV of 23 December 1999 regarding the Security and Intelligence Service of the Republic of Moldova**<br><br>**Article 7.** Functions of the Service<br>The Service shall have the following functions:<br>…….<br>e) to ensure the technical support of the interception of communications conveyed by means of electronic communications networks, with the use of special technical means, connected, if it is necessary, to the equipment of the providers of electronic communications networks and/or services. | **Article I.** – In article 7 letter e) of Law no. 753-XIV of 23 December 1999 regarding the Security and Intelligence Service of the Republic of Moldova (Official Gazette of the Republic of Moldova, 1999, no. 156, article 764), subsequently amended and completed, after the phrase „the technical support of the interception of" the phrase „computer data and of" shall be added. |
| These amendments have editorial character. | **Article II.** – The Criminal Code of the Republic of Moldova no. 985-XV of 18 April 2002 (republished in the Official Gazette of the Republic of Moldova, 2009, no. 72-74, article 195), subsequently amended and completed, shall be amended and completed as follows:<br><br>1 Throughout the Code, the word „telecommunications", in any grammatical case, shall be replaced by the phrase „electronic communications systems", in the respective grammatical case.<br>2. In article 178 paragraph (1), the phrase „telegraphic notices" shall be replaced by the phrase „electronic communications". |
| **The Criminal Code of the Republic of Moldova no. 985-XV of 18 April 2002**<br>**Article 208[1].** Child pornography<br>The production, distribution, dissemination, import, export, offering, selling, purchase, exchange, use or holding of images or other representations of one or more children involved in explicit sexual activities, whether real or simulated, or of images or other representations of a child's sexual organs, depicted in a lascivious or | 3. Article 208[1]:<br>In the provision, after the word „the use" the phrase „ , the deliberate obtaining, by means of information technologies or electronic communications systems, of access to" shall be added;<br>In the sanction, the phrase „from 1 to 3 years" shall be replaced by the phrase „from 3 to 7 years". |

| | |
|---|---|
| obscene manner, including in electronic form,<br>shall be punished with a jail term from 1 to 3 years, with a fine imposed to legal persons from 2000 to 4000 conventional units including the loss of the right to carry out a certain activity. | |
| **Article 259.** The illegal access to computerised information<br>(1) Illegal access to computerised information, that is the information stored in computers, on material storage media, in computer systems or computer networks by a person who is not authorised under the legislation in force or a contract, who exceeds the limits of the authorisation or does not have the permission of the competent person to use, manage or control a computer system or carry out scientific research or perform any other operation in a computer system, if it is accompanied by the destruction, deterioration, alteration, blocking or copying of the information and disruption of the operation of computers, a computer system or computer network and has caused large scale damages,<br>shall be punished with a fine from 200 to 500 conventional units or unpaid community work from 150 to 200 hours or a jail term of up to 2 years, a fine imposed to legal persons from 1000 to 3000 conventional units including the loss of the right to carry out a certain activity.<br>(2) The same action committed:<br>a) by two or more persons;<br>b) by violation of protection systems;<br>c) by connection to telecommunication channels;<br>d) by use of special technical means;<br>e) by illegal use of a computer, computer system or computer network, for the purpose of committing offences referred to in paragraph (1), articles $260^1$–$260^3$, $260^5$ and $260^6$;<br>f) with respect to information protected by the legislation in force;<br>g) in especially large-scale proportions<br>shall be punished with a fine from 500 to 1000 conventional units or unpaid community work from 180 to 240 hours, or a | 4. Article 259:<br>in paragraph (1), the phrase „and has caused large-scale damages” shall be excluded;<br>in paragraph (2), letter h) shall have the following content:<br>,,h) causing large-scale damages”. |

| | |
|---|---|
| jail term of up to 3 years, and legal persons shall be punished with a fine from 3000 to 6000 conventional units including the loss of the right to carry out a certain activity or the dissolution of the legal person. | |
| **Article 260.** The production, import, marketing or making available of technical means or software products<br>The illegal production, import, marketing or making available, in any other form, of technical means or software products, designed or adapted with a view to committing one of the crimes provided for in articles 237, 259, $260^1$–$260^3$, $260^5$ and $260^6$<br>shall be punished with a fine from 500 to 1000 conventional units or a jail term from 2 to 5 years, with a fine imposed to legal persons from 3000 to 6000 conventional units including the loss of the right to carry out a certain activity or the dissolution of an enterprise. | 5. In the sanction of article 260, the phrase „from 500 to 1000 conventional units" shall be replaced by the phrase „from 200 to 500 conventional units", and the phrase „from 2 to 5 years" shall be replaced with the phrase „of up to 3 years". |
| **Article $260^1$.** Illegal interception of a computer data transmission<br>Illegal interception of computer data transmission, including electronic releases that are not public and are destined to a computer system, originate from such a system or are carried out within a computer system<br>shall be punished with a fine from 500 to 1000 conventional units or a jail term from 2 to 5 years, a fine imposed to legal persons from 3000 to 6000 conventional units including the loss of the right to carry out a certain activity or the dissolution of an enterprise. | 6. In the sanction of article $260^1$, the phrase „from 2 to 5 years" shall be replaced by the phrase „of up to 5 years". |
| **Article $260^2$.** The alteration of the integrity of data stored in a computer system<br>The intentional modification, deletion or deterioration of data stored in a computer system or the illegal restriction of the access to this data, the unauthorised transfer of computer data from a computer system or a storage medium, the acquisition, marketing or making available of computer data with limited access, in any form, if these actions have caused large-scale damages,<br>shall be punished with a fine from 500 to 1000 conventional units or a jail term from 2 to 5 years. | 7. Article $260^2$:<br>in the provision, after the word „intentional" the word „unauthorised" shall be inserted, and the phrase „ , if these actions have caused large-scale damages," shall be excluded;<br>in the sanction, the phrase „from 2 to 5 years" shall be replaced by the phrase „of up to 5 years". |
| **Article $260^3$.** The disruption of the functioning of a computer system<br>(1) The disruption of the functioning of a computer system by inserting, transmitting, modifying, deleting or deteriorating computer data or by restricting | 8. Article $260^3$:<br>paragraph (1):<br>in the provision, after the word „deteriorating" the phrase „ ,in an intentional and unauthorised manner, " shall be added, and the phrase „ , if these actions have |

| | |
|---|---|
| access to these data, if these actions have caused large-scale damages,<br>shall be punished with a fine from 700 to 1000 conventional units or unpaid community work from 150 to 200 hours, or a jail term from 2 to 5 years, with a fine imposed to legal persons, from 3000 to 6000 conventional units including the loss of the right to carry out a certain activity or the dissolution of an enterprise.<br>(2) The same action:<br>a) committed out of financial interest;<br>b) committed by two or more persons;<br>c)committed by an organised criminal group or a criminal organisation;<br>d) that has led to especially large-scale damages<br>shall be punished with a fine from 700 to 1000 conventional units or a jail term from 3 to 7 years, with a fine imposed to legal persons, from 3000 to 6000 conventional units or the dissolution of an enterprise. | caused large-scale damages," shall be excluded;<br>in the sanction, the phrase „from 2 to 5 years" shall be replaced by the phrase „of up to 5 years";<br>paragraph (2), letter d) shall have the following content:<br>„d) that has led to large-scale damages". |
| **Article 260[4].** The production, import, marketing or illegal making available of access codes or similar data<br>(1) The illegal production, import, marketing or making available, in any other form, of a password, an access code or of similar data that allow total or partial access to a computer system for the purpose of committing one of the crimes provided for in articles 237, 259, 260[1]–260[3], 260[5] and 260[6], if these actions have caused large-scale damages,<br>shall be punished with a fine from 500 to 1000 conventional units or a jail term from 2 to 5 years, with a fine imposed to legal persons, from 1000 to 3000 conventional units including the loss of the right to carry out a certain activity.<br>(2) The same action:<br>a) committed out of financial interest;<br>b) committed by two or more persons;<br>c) committed by an organised criminal group or a criminal organisation;<br>d) that has led to especially large-scale damages<br>shall be punished with a fine from1000 to 1500 conventional units or a jail term from 3 to 7 years, with a fine imposed to legal persons, from 3000 to 6000 conventional units including the loss of the right to carry out a certain activity or the dissolution of an enterprise. | 9. Article 260[4]:<br>paragraph (1):<br>in the provision, the phrase „ , if these actions have caused large-scale damages," shall be excluded;<br>in the sanction, the phrase „from 2 to 5 years" shall be replaced by the phrase „of up to 3 years";<br>in paragraph (2), letter d) shall have the following content:<br>„d) that have led to large-scale damages". |
| **Article 260[5].** Electronic forgery<br>The illegal insertion, modification or | 10. In the sanction of article 260[5], the phrase „ from 2 to 5 years" shall be replaced |

| | |
|---|---|
| deletion of computer data or the illegal restriction of the access to these data, resulting in data contrary to truth, for the purpose of being used in order to produce legal consequences<br>shall be punished with a fine from 1000 to 1500 conventional units or a jail term from 2 to 5 years. | by the phrase „of up to 5 years”. |
| **Article 260[6].** Electronic fraud<br>(1) The illegal insertion, modification or deletion of computer data, the illegal restriction of the access to these data or the hindering in any way of the functioning of a computer system, in order to gain financial benefits for oneself or someone else, if these actions have caused large-scale damages,<br>shall be punished with a fine from 1000 to 1500 conventional units or unpaid community work from 150 to 200 hours, or a jail term from 2 to 5 years.<br>(2) The same actions:<br>a) committed by an organised criminal group or a criminal organisation;<br>b) that have led to especially large-scale damages<br>shall be punished with a jail term from 4 to 9 years. | 11. Article 260[6]:<br>paragraph (1):<br>in the provision, before the word „insertion”, the phrase „intentional and unauthorised” shall be introduced, and the phrase „ if these actions have caused large-scale damages,” shall be excluded;<br>in the sanction, the phrase „from 2 to 5 years” shall be replaced with the phrase „of up to 5 years”;<br>paragraph (2):<br>in the provision, letter b) shall have the following content:<br>,,b) that have led to large-scale damages ”;<br>In the sanction, the phrase „from 4 to 9 years” shall be replaced with the phrase „from 4 to 10 years”;<br>Shall be completed with paragraph (3) as follows:<br>„(3) The actions provided for in paragraph (1) or (2) of this article, that have led to especially large-scale damages,<br>shall be punished with a jail term from 8 to 15 years.” |
| **Article 261[1].** Unauthorised access to telecommunications networks and services<br>(1) Unauthorised access to telecommunications networks and/or services by using the telecommunications networks and/or services of other operators, if this has led to large-scale damages,<br>shall be punished with a fine from 500 to 1000 conventional units or a jail term of up to 1 year and legal persons shall be punished with a fine from 1000 to 3000 conventional units including the loss of the right to carry out a certain activity.<br>(2) The same action:<br>b) committed by two or more persons;<br>c) committed by violating protection systems;<br>d) committed by using special technical means;<br>e) that has led to especially large-scale damages<br>shall be punished with a fine from 1000 | 12. Article 261[1]:<br>paragraph (1):<br>in the provision, phrase „ , if this has led to large-scale damages,” shall be excluded;<br>in the sanction, the phrase „of up to 1 year” shall be replaced with the phrase „of up to 2 years”;<br>paragraph (2):<br>in the provision, letter e) shall have the following content:<br>„e) that has led to large-scale damages”. |

| | |
|---|---|
| to 3000 conventional units or a jail term of up to 5 years, and legal persons shall be punished with a fine from 3000 to 6000 conventional units including the loss of the right to carry out a certain activity. | |
| The norm is new and is not comprised in the current legislation | **Article III.** – The Code of Criminal Procedure of the Republic of Moldova no. 122-XV of 14 March 2003 (republished in the Official Gazette of the Republic of Moldova, 2013, no. 248-251, article 699), subsequently amended and completed, shall be amended and completed as follows:<br><br>1. The Code shall be completed with article $130^1$ having the following content:<br>„Article $130^1$. Computer data search and seizure of objects containing computer data<br>(1) Computer search means the process of looking for, researching, discovering, identifying and accumulating computer data existing in a computer system or computer data storage medium that are relevant for the criminal case, carried out through technical methods and means that ensure the integrity and authenticity of the information contained thereon.<br>(2) Computer search shall be carried out following a reasoned ordinance of the criminal investigation body and only upon authorisation by the investigating magistrate.<br>(3) While carrying out the computer search and/or seizure of objects containing computer data, the presence of the person subject to the search and/or seizure or of adult members of their family or of those who represent their interests must be guaranteed. If the presence of these persons is not possible, the representative of the executorial authority of the local public administration shall be invited.<br>(4) The computer search and the seizure of objects containing computer data at the premises of state institutions, enterprises, organisations and military units shall be carried out in the presence of this representative.<br>(5) In the case in which, during the search of a computer system or of a computer data storage medium, it is established that the searched computer data are partially or entirely contained in another computer system or computer data storage medium and are legally accessible from the system or medium initially searched or are available for the |

| | |
|---|---|
| | system or medium initially searched, the search of the other computer system or data storage medium may be carried out following a reasoned ordinance of the prosecutor, without the authorisation of the investigating magistrate, under the obligation to submit immediately to the latter, no later than 24 hours from the conclusion of the computer search, the computer data obtained in result, indicating the reasons for its carrying out. The investigating magistrate checks the legality of this procedural action.<br>(6) In the case of establishing that the computer search carried out under the terms of article (5) of this article has been legally conducted, the investigating magistrate shall confirm its results in a reasoned conclusion. Otherwise, in a well-founded ruling, they shall acknowledge the search of the other computer system or storage medium to be illegal.<br>(7) In the case in which, the seizure of the objects containing computer data may seriously affect the authorised provision of public electronic communication networks and services, the criminal investigation body shall order through a reasoned ordinance, the copying of these computer data. In other cases, in which the respective objects are not used for the authorised provision of public electronic communication networks and services, but their seizure might seriously affect the activity of the person who owns or controls them, the criminal investigation body may order, through a well-founded ordinance, the copying of these computer data. The given copies shall serve as means of evidence and shall be made using technical means and methods that ensure the integrity and authenticity of computer data.<br>(8) In the case in which, the carrying out of the computer search requires a long term, the person in charge of the criminal investigation shall seize the objects containing computer data in order to examine them at the premises of the criminal investigation body. For this purpose, the objects containing computer data shall be packed and sealed and the package shall be signed and the corresponding mention shall be introduced in the minutes.<br>(9) In addition to the provisions of article 260, the minutes regarding the computer search must comprise information on:<br>a) the description and listing of |

| | |
|---|---|
| | computer systems or computer data storage media subject to the search;<br>b) the description and listing of the activities carried out;<br>c) the description and listing of computer data discovered during the computer search.<br>(10) the computer search and the seizure of the objects containing computer data shall be carried out in accordance with the provisions of this Code." |
| **LAW**<br>**The Code of Criminal Procedure of the Republic of Moldova**<br>**(General part)**<br><br>**no. 122-XV of 14.03.2003**<br>……..<br>**Section 5**<br>**Special investigation activity**<br>**Section 5**<br>**Special investigation activity**<br>**Article 132[1].** General provisions regarding the special investigation activity<br>(2) Special investigation measures shall be ruled and carried out if the following conditions are altogether met:<br>1) the purpose of the criminal process cannot be achieved another way and/or the activity of administering the evidence can be considerably prejudiced;<br>2) there is a reasonable suspicion with respect to the preparing or commission of a serious, especially serious or exceptionally serious crime, with the exceptions established by law;<br>3) the measure is necessary and proportional to the restriction of fundamental human rights and liberties.<br><br>Article 132[6]. The inspection of the domicile and/or installation there of devices ensuring audio and video surveillance and record, and of photo and video cameras<br>Article 132[7]. The surveillance of the domicile through the use of recording technical devices<br>Article 133. The retention, inspection, delivery, search or seizure of mail<br>Article 134[4]. The collecting of information from the provider of electronic communications services<br>Article 134[5]. The identification of the | 2. The articles shall be completed as follows: 132[6] – with paragraph (6), 132[7] and 134[3] – with paragraph (3), 133 – with paragraph (7), 134[5] – with paragraph (5), 134[4], 134[6] and 138[3] – paragraph (2), 136 – paragraph (9), and in article 138[1], paragraph (5) shall be amended, all paragraphs having the following contents:<br>„The special investigation measure provided for by this article may be ruled in the case provided for in article 132[1] paragraph (2) point. 2) of this code or of an offence provided for in articles 174-175[1], 185[1]-185[3], 208[1], 208[2], 237 and 259-261[1] of the Criminal Code." |

| | |
|---|---|
| subscriber, owner or user of an electronic communication system or of an access point to a computer system<br>Article 134[6]. Visual pursuits<br>Article 136. Undercover investigation<br>Article 138[1]. Cross border surveillance<br>Article 138[3]. Control acquisition<br><br>**L AW**<br>**The Criminal Code of the Republic of Moldova no. 985-XV of 18 April 2002**<br><br>Article 174. Sexual relation with a person below the age of 16<br>Article 175. Perverse actions<br>Article 175[1]. Accosting children for sexual purposes<br><br>**Chapter V**<br>**CRIMES AGAINST POLITICAL, LABOUR AND OTHER CONSTITUTIONAL RIGHTS OF CITIZENTS**<br>Article 185[1]. Violation of copyright and related rights<br>Article 185[2]. Violation of the right over industrial property objects<br>Article 185[3]. Intentionally forged statements in Incorporation papers with respect to the protection of intellectual property<br><br>**Chapter VII**<br>**CRIMES AGAINST FAMILY AND MINORS**<br>Article 208[1]. Child pornography<br>Article 208[2]. Resorting to prostitution practiced by a child<br><br>**Chapter X**<br>**ECONOMIC CRIMES**<br>Article 237. Manufacturing and circulation of forged cards or other payment instruments<br><br>**Chapter XI**<br>**CYBERCRIMES AND TELECOMMUNICATION CRIMES**<br>Article 259. Illegal access to computer information<br>Article 260. Production, import, marketing or illegal making available of technical devices or software<br>Article 260[1]. Illegal interception of computer data transmission<br>Article 260[2]. Alteration of computer data integrity held within a computer system<br>Article 260[3]. Disruption of computer system operation | |

| | |
|---|---|
| Article 260[4]. Production, import, marketing or illegal provision of passwords, access codes or similar data<br>Article 260[5]. Electronic forgery<br>Article 260[6]. Electronic fraud<br>Article 261. Violation of computer system security rules<br>Article 261[1]. Unauthorised access to telecommunication networks and services | |
| **L A W**<br>**Code of Criminal Procedure of the Republic of Moldova**<br>**(General Part)**<br><br>**no. 122-XV of 14.03.2003**<br><br>**Article 138[2].** Controlled delivery<br><br>**Article 132[1].** General provisions on the special investigation activity<br>(1) Special investigation activities shall be required and carried out if the following conditions are jointly met:<br><br>2) There is a reasonable suspicion regarding the preparation or commission of a serious, extremely serious or exceptionally serious crime, with the exceptions provided by law;<br><br>**L AW**<br>**The Criminal Code of the Republic of Moldova no. 985-XV of 18 April 2002**<br><br>Article 175[1]. Accosting children for sexual purposes | 3. Article 138[2] shall be completed with paragraph (7) having the following content:<br>„The special investigation measure provided for in this article may be ruled in the case of offences provided for in article 132[1] paragraph (2) point 2) of this code or of an offence provided for in articles 175[1], 185[1]-185[2], 208[1], 208[2], 237, 260-260[2], 260[4], 260[6] and 261[1] of the Criminal Code.” |

| | |
|---|---|
| **Chapter V**<br>**CRIMES AGAINST POLITICAL, LABOUR AND OTHER CONSTITUTIONAL RIGHTS OF CITIZENTS**<br>Article 185[1]. Violation of copyrights and related rights<br>Article 185[2]. Violation of the right over industrial property objects<br><br>**Chapter VII**<br>**CRIMES AGAINST FAMILY AND MINORS**<br>Article 208[1]. Child pornography<br>Article 208[2]. Resorting to prostitution practiced by a child<br><br>**Chapter X**<br>**ECONOMIC CRIMES**<br>Article 237. Manufacturing and circulation of forged cards or other payment instruments<br><br>**Chapter XI**<br>**CYBERCRIMES AND TELECOMMUNICATION CRIMES**<br>Article 260. Production, import, marketing or illegal making available of technical devices or software<br>Article 2601. Illegal interception of computer data transmission<br>Article 2602. Alteration of computer data integrity held within a computer system<br>Article 2604. Production, import, marketing or illegal provision of passwords, access codes or similar data<br>Article 2606. Electronic fraud<br>Article 2611. Unauthorised access to telecommunication networks and services | |
| **Article 132[2].** Special investigation measures<br>(1) In order to uncover and investigate crimes, the following special measures shall be undertaken:<br>1) upon authorisation of the investigating magistrate:<br>……<br>d) retention, inspection, handing over, search or seizure of mail; | 4. Article 132[2] paragraph (1) point 1):<br>Shall be completed with letter c[1]) having the following content:<br>„c[1]) interception and recording of computer data";<br>In letter d), after the phrase „mail" the phrase "and electronic communications" shall be inserted. |
| **Article 132[8].** Interception and recording of communications<br>…….<br>Article 174. Sexual relation with a person below the age of 16 | 5. In article 132[8] paragraph (2), after the phrase „article 172 paragraphs (2) and (3)" the phrase „ , article 174," shall be added. |
| | 6. Article 132[11] shall have the following |

| | |
|---|---|
| Article 132[8]. Interception and recording of communications<br>Article 132[9]. Carrying out and certification of the interception and recording of communications<br>Article 132[10]. Recording of images<br>Article 132[11]. Interception and recording of computer data | content:<br>„Article 132[11]. Interception and recording of computer data<br>(2)The interception and recording of computer data consists in the use of technical methods and/or means through which are collected in real time the data referring to the cyber traffic and/or data related to contents, associated to the given communications, other than those provided for in article 132[8], transmitted through a computer system, and the storage of information obtained following interception on a technical medium.<br>(2) The interception and recording of computer data shall be ordered and carried out under the conditions stated in article 132[9], which shall be correspondingly enforced.<br>(3) The special investigation measure provided for by this article may be ordered in the case of the offences provided for in article 132[1] paragraph (2) point 2) of this code or of an offence provided for in articles 175-175[1], 185[1]-185[3], 208[1], 208[2], 237 and 259-261[1] of the Criminal Code.” |
| The norm is new and is not comprised in the current legislation. | 7. The law shall be completed with article 132[12] having the following content:<br>„Article 132[12]. Check of the interception recordings<br>Evidence means obtained under the conditions of articles 132[8]-132[11] may be checked through technical expertise, ruled by a court on the request of the parties or ex officio.” |
| These amendments have editorial character. | 8. Article 133:<br>in the title, after the phrase „of mail” the phrase „and of electronic communications” shall be added;<br>in paragraph (1), after the phrase „mail” the phrase „and/or electronic communications” shall be inserted;<br>in paragraph (2), after the phrase „mail” the phrase „and/or electronic communications” shall be added, and after the word „fax” the phrase „ , text messaging through computer systems other than telephony services” shall be added;<br>in paragraph (3), after the phrase „mail” the phrase „and/or electronic communications” shall be added, after the phrase „of the postal institution” the phrase „or, as appropriate, of the provider of email or text messaging services” shall be added and after the phrase „mail” the phrase „and/or |

| | |
|---|---|
| | electronic communications" shall be added;<br>in paragraph (4), after the phrase „of the postal institution" the phrase „or, as appropriate, of the provider of email or text messaging services" shall be inserted;<br>in paragraph (5), after the phrase „of the postal institution" the phrase „or, as appropriate, of the provider of email or text messaging services" shall be inserted;<br>in paragraph (6), after the phrase „of mail" the phrase „and/or of electronic communications" shall be inserted.<br><br>9. Article 134 shall be completed with paragraph (4) having the following content:<br>„ (4) The provisions of paragraphs (1)-(3) of this article shall be enforced correspondingly in the case of information related to electronic communications, too." |
| **Article 134.** Examination and seizure of mail<br>(1) Upon presentation at the postal institution, the representative of the criminal investigation body shall inform the head of the institution, who shall be under obligation of signing the given notice, about the ordinance regarding the examination and seizure of mail, shall open and examine the mail.<br>(2) When documents and objects with probative value in the criminal investigation are detected, the representatives of the criminal investigation body shall seize or make copies thereof. In the absence of such documents and objects, the representative of the criminal investigation body shall order the delivery of the inspected mail to its addressee.<br>(3) Under the provisions of articles 260 and 261, minutes shall be taken on each mail examination or seizure, indicating, in particular, who, where and when has examined and seized the mail, ordered the delivery thereof to the addressee, as well as the type of mail, and mails that copies were made of, technical means used and what has been detected. All the participants and those present at this procedural action shall be warned on the obligation of keeping the secrecy of correspondence, non-disclosure of the information concerning the criminal investigation, as well as on the criminal liability provided for in articles 178 and 315 of the Criminal Code. These facts shall be | 9. Article 134 shall be completed with paragraph (4) having the following content:<br>„ (4) The provisions of paragraphs (1)-(3) of this article shall be enforced correspondingly in the case of information related to electronic communications, too." |

| | |
|---|---|
| recorded in the minutes. | |
| | 10. Article $134^2$ paragraph (2):<br>after number „$165^1$" the phrase „ , $175^1$, $185^1$-$185^2$" shall be inserted;<br>number „208" shall be replaced by the phrase „208-$208^2$";<br>after number „256" the phrase „, 259-$261^1$" shall be inserted. |
| | 11. In article $134^5$ paragraph (1), the word „telecommunications" shall be replaced by the phrase „electronic communications". |
| | 12. In article 305 paragraph (3), after the phrase „upon interception and recording of communications" the phrase „, upon interception and recording of computer data" shall be added. |
| **LAW**<br>**regarding the practice of the medical profession**<br>**no. 264-XVI of 27.10.2005**<br><br>**Article 17.** Professional obligations of the doctor<br>The doctor is obliged to:<br><br>The norm is new and is not comprised in the current legislation. | **Article IV.** – In article 17 of Law no. 264-XVI of 27 October 2005 regarding the practice of the medical profession (Official Gazette of the Republic of Moldova, 2005, no. 172-175, article 839), subsequently modified and completed, paragraph (1) shall be completed with letter $e^1$) having the following content:<br>„$e^1$) to transmit to the law enforcement bodies any information, they have learnt about in the exercise of their job duties, regarding abuse cases and violence, including sexual ones and those directed towards children". |
| | **Art. V.** – In article 20 of the Law on electronic communications no. 241-XVI of 15 November 2007 (Official Gazette of the Republic of Moldova, 2008, no. 51-54, article 155), subsequently modified and completed, paragraph (3) shall be amended as follows:<br>in letter a), the word "operative" shall be replaced by the word „special";<br>in letter b), the word „operative" shall be replaced by the word „special". |
| | **Art. VI.** – Contravention Code of the Republic of Moldova no. 218-XVI of 24 October 2008 (Official Gazette of the Republic of Moldova, 2009, no. 3-6, article 15), subsequently completed and amended, shall be amended and completed as follows:<br><br>1. The provision of article 90 shall be completed in the end with the phrase „, or their deliberate accessing in public places". |

| | |
|---|---|
| | 2. Shall be completed with article 247[1] having the following content:<br>„Article 247[1]. The breach of the legislation regarding the prevention and combating of cyber crimes<br>The breach of the legislation regarding the prevention and combating of cyber crimes by the providers of electronic communications services, regardless of the type of ownership or legal form of organisation, expressed through:<br>a) failure to fulfil the obligation to keep the record of service users;<br>b) failure to communicate to the competent authorities the illegal access to the information in the computer system, the attempts to introduce illegal programmes, the violation by responsible persons of the rules for the collection, processing, storage, dissemination and distribution of information or of the rules regarding the protection of the computer system established in agreement with the status of the information or with its degree of protection, if these have contributed to the appropriation, distortion or destruction of information or have led to other serious repercussions, the disturbance of the functioning of computer systems, other computer security incidents with a significant impact;<br>c) failure to comply, in confidence, with the request of the competent authority with regard to the rapid preservation of computer data or of the data referring to the information traffic, indicated in the respective request, which are in danger of destruction or alteration, under the conditions established by law;<br>d) failure to submit to the competent authorities, following a request made under the terms of procedural legislation, of the data referring to information traffic or users;<br>e) failure to enforce security measures through the employment of certain procedures, devices or specialised softwares with which the access to the user's own computer system might be restricted or forbidden without such a right;<br>f) failure to ensure the preservation of data referring to the traffic, under the conditions established by law, in order to identify service providers, service users and the channel through which the communication has been transmitted;<br>g) failure to fulfil the obligation to stop, using owned technical methods and means, |

| | |
|---|---|
| | under the conditions established by law, the access to all IP addresses where web pages are located, including those hosted by the respective provider, which contain child pornography, promote sexual abuse or sexual exploitation of children, contain information propagating war or terrorism, incite to national, racial or religious hate or discrimination, to hostility or violence, contain or disseminate instruction concerning the manner of committing crimes,<br>shall be sanctioned with a fine from 100 to 150 conventional units imposed to natural persons and a fine from 400 to 500 conventional units imposed to legal persons."<br><br>3. Article 252 shall be excluded.<br><br>4. In article 400 paragraph (1), after the number „245" the text „, 247[1]" shall be introduced. |
| | **Article VII.** – Law no. 20-XVI of 3 February 2009 regarding the prevention and combating of cyber crimes (Official Gazette of the Republic of Moldova, 2010, no. 11-12, article 17), subsequently amended and completed, shall be amended and completed as follows:<br><br>1. Article 2 shall be completed with the following notions:<br>*„critical infrastructure* – an element or a system, located on the territory of the state, which is essential for maintaining the functions of ensuring the health, security, social, economic and other kinds of welfare of the population, which disturbance or destruction may have a negative impact, as a result of the incapacity to carry along these functions;<br>*owner/operator/administrator of the critical infrastructure* – any entity established by Government to be the holder of an element or of a system that is part of the critical infrastructure or is in charge of its operation/administration;<br>*preservation of data* – the keeping and protection of the integrity of the data existing in a computer system, owned and controlled by a person;<br>*computer data security* – a state of normality resulted from implementing a set of measures through which confidentiality, integrity, availability and authenticity of |

| | |
|---|---|
| | computer data and public or private services and resources are guaranteed, including by preventing and combating cyber criminality;<br>*Computer security incident* – a disruption of computer security that has or may have a negative impact on keeping the confidentiality, integrity, availability and authenticity of electronic information and public or private resources or services;<br>*Cyber criminality* – negative social phenomena characterised by a set of criminal activities in which computer data and/or computer systems are an instrument for the commission of the crime or an object of the crime."<br><br>2. Article 4 shall have the following content:<br>"Article 4. Responsibilities of law enforcement bodies in preventing and combating cyber criminality.<br>(1)The framework of the Prosecutor General`s Office, the General Police Inspectorate of the Minister for Internal Affairs and the Security and Intelligence Service shall comprise specialized divisions, whose responsibilities shall include preventing and combating cyber criminality and which shall work together to fulfil the given responsibilities.<br>(2) The General Police Inspectorate shall carry out the activity of preventing and combating cyber criminality, in accordance with the legislation in force, including through special investigative activity and the conduct of criminal investigation in cyber criminality cases, an order regarding the rapid preservation of computer data or data related to information traffic, the appointment of a contact point responsible for ensuring international cooperation in combating cybercrime, the carrying out of international cooperation, the analysis of the cyber criminality trend and the identification and protection of cyber criminality victims.<br>(3) The General Police Inspectorate and the Security and Intelligence Service, with the participation of other public authorities and private institutions shall develop, manage and update by means of an automatic information system, databases on the phenomenon of cyber criminality.<br>(4) The General Police Inspectorate and the Prosecutor General`s Office shall jointly carry out studies aimed at detecting and eliminating the causes and conditions that |

| | |
|---|---|
| | favour cyber criminality and publish their results through mass media.<br>(5) The Prosecutor General`s Office:<br>a) shall carry out, within the limits of its competence, activities of prevention and combating of cyber criminality, in accordance with the current legislation;<br>b) shall coordinate, lead and conduct the criminal investigation in cyber criminality cases;<br>c) shall represent in court the accusation on behalf of the state;<br>d) shall receive and transmit requests for international legal assistance, extradition or provisional detention made at the criminal investigation stage;<br>e) shall order during the criminal investigation stage, upon request of the criminal investigative body or ex officio, rapid preservation of computer data or data relating to information traffic, which are in danger of destruction or alteration, under the conditions of criminal procedure legislation;<br>f) shall take other measures aimed at preventing and combating cyber criminality.<br>(6) The Security and Intelligence Service shall perform activities aimed at preventing and combating cyber criminality that pose threats to national security, including special investigation work, revealing activity of international criminal groups and organisations, other activities within its competence.<br>(7) The National Institute of Justice shall carry out the personal development of the staff engaged in the administration of justice in the fight against cyber criminality."<br><br>3. The law shall be completed with article $4^1$ having the following content:<br><br>Article $4^1$. The National Plan for preventing and combating cyber criminality<br>(4) In order to prevent and combat cyber criminality, as well as to ensure the protection of its victims, the Government shall approve the National Plan for preventing and combating cyber criminality (hereinafter the National Plan), drawn up with consideration of the opinion of the Prosecutor General`s Office.<br>(5) The National Plan shall be approved periodically, for a three years term and shall provide for the implementation of |

| | |
|---|---|
| | complex actions, the carrying out of socio-economic initiatives aimed at preventing and combating cyber criminality as well as protecting its victims, including through cooperation with international organisations, nongovernmental organisations, other institutions and representatives of civil society.<br>(6) Central public administration authorities responsible for preventing and combating cyber criminality, shall adopt their own action plans to implement the National Plan in their own fields of activity.<br>(7) Article 5 shall be completed with paragraph (2) having the following content:<br>"Service providers, nongovernmental organisations, civil society representatives and other persons shall be encouraged to communicate to the General Police Inspectorate or to the Prosecutor General`s Office any information they have learnt with respect to private or legal persons who share, disseminate, import or export images containing representations of one or more children involved in sexual activities and also with respect to sexual abuse of children committed through electronic communications."<br>The law shall be completed with article $6^1$ having the following content:<br>Article $6^1$. Obligations of owners and operators of critical computer infrastructures.<br>In order to prevent cyber criminality, owners and operators of critical computer infrastructures are obliged to:<br>d) implement the minimum requirements established by the responsible state authority with respect to the security of owned or operated critical computer infrastructures.<br>e) create a contact point in order to interact with public authorities and state institutions empowered to ensure the security of critical computer infrastructures.<br>f) cooperate with the competent authorities in ensuring the security of critical computer infrastructures owned or operated. |

| | |
|---|---|
| | d) communicate immediately to the competent authorities, no later than 24 hours from the moment of detection, information about the illegal access to their own computer data system, attempts to introduce illegal programmes, the violation by responsible persons of the rules regarding collection, processing, storage, dissemination and distribution of information or of the rules regarding the protection of the computer system established in agreement with the status of the information or with its degree of protection, if these acts have contributed to the appropriation, distortion or destruction of information or have led to other serious repercussions, the disruption of the functioning of computer systems, other computer security incidents with a significant impact."<br><br>6. Article 7:<br>Paragraph (1):<br>Letter a) shall be completed at the end with the phrase: "and in case of prepaid anonymous services – date and time of the first activation of service";<br>in letter b), the phrase "data about information traffic, inclusively" shall be substituted with the phrase: ", provided by article 4, paragraph(1),", and the words "information delicts" shall be replaced by the words "information security incidents with significant impact";<br>in letter c), the word "immediate" shall be replaced by the word "rapid", after the words "information traffic" the text shall be introduced, as follows: ", indicated in the respective request", and the phrase "120 calendar days" shall be replaced by the phrase "180 calendar days";<br>in letter d), the words "of the law" shall be replaced by "procedural legislation", and after the word "relating" the words "to information traffic and" shall be introduced;<br>in letter e), the word "a" shall be replaced by the words "its own", and the word "unauthorised" shall be replaced by the words "without such a right";<br>in letter f), the text "monitoring, surveillance and" shall be excluded, and the phrase "for a period of 180 calendar days" shall be replaced by the phrase "in fixed and mobile telephony network for a period of one year, and of those relating to Internet traffic and Internet telephony – for a period of 6 months"; |

| | |
|---|---|
| | in letter g), after the word “network” the text ”based on the request of the competent authority referred to in article 4, paragraph (1), within the limits of its technical performances,”;<br>letter h) shall be added, with the following content:<br>h) to stop, under the provisions of the law, from own computer system, using available technical methods and means, the access to all IP addresses on which web pages are located, including those hosted by the concerned provider, which contain child pornography, promote sexual abuse or child sexual exploitation, contain information which propagates war or terrorism, urges to hatred and national, racial or religious discrimination, to hostility or violence, contain or disseminate instructions on how to commit crimes”,<br>in the paragraph (2), the word “immediately” shall be replaced by the words “in reasonable terms”.<br>7. Article 10:<br>In paragraphs (1) and (2), the word “immediate” shall be replaced by the word “quick”;<br>paragraph (5) shall be added, as follows:<br>“(5) If the competent authority from the Republic of Moldova finds out that a service provider, had, while executing a request of traffic-related data preservation, participated in the transmission of this communication in another state, it shall rapidly disclose to the requesting foreign competent authority an adequate amount of traffic-related data, in order to identify the service provider and the channel the information was transmitted thereby.” |
| | **Art. VIII.** – Article 18 para. (1) point 1) from Law no. 59 of 29 March 2012 on the special investigation activity (Official Gazette of the Republic of Moldova, 2012, nos. 113-118, art. 373), with further amendments and completions, shall be completed as follows:<br>Letter $c^1$ shall be added, as follows:<br>„$c^1$) interception and recording of information data”;<br>in letter d), after the words “of mails”, the phrase “and/or electronic communications” shall be added.<br><br>**Chairman of Parliament** |