Strasbourg, 25 November 2016

CDL-AD(2016)039
Or. Engl

Opinion no. 859/2016

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

REPUBLIC OF MOLDOVA

JOINT OPINION

OF THE VENICE COMMISSION AND OF THE DIRECTORATE GENERAL OF HUMAN RIGHTS AND RULE OF LAW (DGI) OF THE COUNCIL OF EUROPE

ON THE DRAFT LAW N° 161 AMENDING AND COMPLETING MOLDOVAN LEGISLATION IN THE FIELD OF CYBERCRIME

Adopted by the Venice Commission at its 109th Plenary Session (Venice,9-10 December 2016)

On the basis of comments by

Mr Iain CAMERON (Member, Sweden)
Mr Jørgen Steen SØRENSEN (Member, Denmark)
Mr Ben VERMEULEN (Member, the Netherlands)
Mr Ian LEIGH (Expert DHR, Human Rights National Implementation Division, United Kingdom)
Ms Sophie STALLA BOURDILLON (Expert DHR, Media Co-operation Unit, United Kingdom
Ms Ioana ALBANI (Expert DGI, Cybercrime Division, Romania)
Ms Cristina SCHULMAN (Expert DGI, Cybercrime Division, Romania)

TABLE OF CONTENTS

I. Introduction

1. By a letter dated 30 June 2016, the authorities of the Republic of Moldova requested the opinion of the Venice Commission on draft law N° 161 amending and supplementing certain legislative acts in the area of preventing and combating cyber criminality (CDL-REF(2016)058), hereinafter "the draft law". The Commission was subsequently informed that, following consultations at domestic level, a number of additional amendments have been introduced in the text in the draft law.

2. Mr I. Cameron, Mr B. Vermeulen and Mr J.S. Sørensen acted as rapporteurs on behalf of the Venice Commission.

3. Ms Albani, Mr Leigh, Ms Schulman and Ms Stalla Bourdillon analysed the draft amendments on behalf of the Directorate General Human Rights and Rule of law ("the Directorate").

4. On 2-3 November 2016, a joint delegation visited the Republic of Moldova and held meetings with representatives of the authorities (Government, Parliament, the Prosecutor General's Office, the Moldovan Intelligence and Security Service), as well as with representatives of the civil society and of international organizations present in the Republic of Moldova. The delegation is grateful to the Moldovan authorities and to other stakeholders met for the excellent co-operation during the visit.

5. This Opinion is based on the English translation of the draft law provided by the Moldovan authorities, which may not accurately reflect the original version on all points. Some of the issues raised may therefore find their cause in the translation rather than in the substance of the provisions concerned.

6. The present joint opinion of the Venice Commission and the Directorate, which was prepared on the basis of the comments submitted by the experts above, was adopted by the Venice Commission at its 109th Plenary Session (Venice, 9-10 December 2016).

II. Preliminary remarks

A. Background

7. According to the accompanying Information Note, the purpose of the draft law is to amend and complete, in the light of applicable European standards, a number of legal acts regulating Moldova's policy in the area of information security protection and fight against cybercrime, as well as against on-line sexual exploitation and abuse of children. The draft law, initiated by the Ministry of Internal Affairs, is intended at the same time to address shortcomings in the implementation of the existing legal framework, and to contribute to implementing more effectively the obligations undertaken by the Moldovan state in this field.

8. The draft law is aimed at amending the following laws:

- Law no. 753-XIV of 23 December 1999 on the Security and Intelligence Service (hereinafter " the law on the Service"), as subsequently amended and completed;
- Criminal Code no. 985-XV of 18 April 2002, as subsequently amended and completed;
- Code of Criminal Procedure no. 122-XV of 14 March 2003, as subsequently amended and completed (hereinafter "CCP");
- Law regarding the practice of the medical profession no. 264-XVI of 27.10.2005;
- Law on electronic communications no. 241-XVI of 15 November 2007;
- Law on preventing and combating cybercrime No. 20-XVI of 03.02.2009 (hereinafter "the Cybercrime Law");
- Contravention Code of the Republic of Moldova no. 218-XVI of 24 October 2008.

- Law n° 59 of 29 March 2012 on the special investigation activity, as amended

9. The Council of Europe and the Venice Commission had carried out previous relevant expert assessments, in 2016, 2008 and 2014.[1]

10. In 2014, the Venice Commission adopted an Opinion on the draft law on amending and supplementing certain legislative acts, promoted by the intelligence and security service of the Republic of Moldova, jointly prepared with the Directorate General of Human Rights (DHR) and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe,[2] (hereinafter the 2014 Joint Opinion). The draft law aimed at establishing a procedure for granting the Service authority to carry out special investigative activities outside criminal law (so-called "security mandate") under the supervision of a judge. The background for the preparation of this draft law was the judgment of the European Court of Human Rights (ECtHR) in the case of *Iordachi and Others v. Moldova* of 14 September 2009[3], in which the Court found that "…*the system of secret surveillance in Moldova is, to say the least, overused, which may in part be due to the inadequacy of the safeguards contained in the law*". More specifically the Court found that the Moldovan law did not provide adequate protection against abuse of power by the State in the field of interception of telephone communications and that the interference with the applicants´ rights under Article 8 of the European Convention of Human Rights was not "in accordance with the law".

11. The 2014 Opinion concluded inter alia that, while it might be legitimate for the Moldovan authorities to wish to establish such a "security mandate", certain matters deserved further consideration, and highlighted in particular the thresholds for initiating security investigations, the relationship between such investigations and evidence gathering in criminal cases, the provision of a four-hour timeframe for deciding requests for security mandates and the effects of security measures not only on the targets of these measures but also on third parties.

12. The purpose of the present joint Opinion is not to address in an exhaustive and detailed manner all provisions of the draft law but to raise the main issues which, in the view of the Commission and the Directorate would require further consideration. The difficulties in separating consideration of the draft law and the legislation to be amended from the wider legal framework - in particular in relation to activities of the Intelligence and Security Service of the Republic of Moldova - should be noted. At the same time, it is important to point out that this Opinion provides an assessment of Draft law N°161. Nothing in the present Opinion should be seen as prejudging the merits or demerits of related legislative provisions in other pending draft laws which will be assessed by the Venice Commission and the Directorate in the future, in particular Draft Law N° 281, which should be seen together with other pending draft laws and the existing framework.

13. Moreover, the joint delegation was informed during the visit to Chisinau that, following discussions with concerned Moldovan stakeholders, additional amendments had been introduced by the Government, amendments which had not been included in the draft law submitted to the Council of Europe for assessment. Hence, it was not possible to provide a detailed assessment, in the present Opinion, of all additional amendments, although these have been taken into account as background information.

---

[1] In 2006, the Council of Europe issued a Review of the 1994 Law on Operative Investigations, in the meantime replaced by the 2012 Law on Special Investigative Activity. The personal data protection issues raised by the Law on the Service were addressed in a separate Opinion issued on 20 February 2006 by an independent expert commissioned by the Directorate General of Legal Affairs of the Council of Europe. In 2008, the Venice Commission gave an Opinion on the Law on State Secret of the Republic of Moldova (see CDL-AD(2008)008, Opinion on the Law on State Secret of the Republic of Moldova, Venice, 14-15 March 2008).

[2] CDL-AD(2014)009, Joint Opinion of the Venice Commission and the Directorate General of Human Rights (DHR) and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the draft law on amending and supplementing certain legislative acts, promoted by the intelligence and security service of the Republic of Moldova, Venice, 21-22 March 2014

[3] *Iordachi and Others v. Moldova,* Application no. 25198/02, judgment of 14 September 2009, §52

B. Standards

14. The draft law has been considered in the light of applicable European norms and principles, notably those enshrined in the European Convention on Human Rights (ECHR) and related case-law, taking into account the particular relevance of Articles 8 and 10 ECHR, as well as of the recommendations contained in the 2014 Joint Opinion, and prior work of the Venice Commission of relevance for the present analysis. This includes the Venice Commission Reports on the Democratic Oversight of Signals Intelligence Agencies,[4] the Report on the Democratic Oversight of the Security Services,[5] as well as the opinions it recently adopted in respect of Poland[6] and Turkey[7] on related matters.

15. Particular attention was paid to the conformity of the proposed draft law with more specific applicable instruments, including :

- the Council of Europe Convention on Cybercrime[8] (hereinafter "the Budapest Convention");
- the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[9] (the Lanzarote Convention);
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce);
- the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (the Data Retention Directive);
- the Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA;
- the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection;
- the Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

16. It is important to point out further that, in the framework of the implementation of the Association Agreement with the EU,[10] the Republic of Moldova committed itself to modifying its legal framework in accordance with the decision of the Court of Justice of the European Union (CJEU) of 8 April 2014, which declared the *Data Retention Directive* invalid, on the grounds that the retention scheme enshrined therein was not in line with Articles 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the EU

[4] CDL-AD(2015)011, Report on the Democratic Oversight of Signals Intelligence Agencies, 20-21 March 2015)

[5] CDL-AD(2015)010, Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007) and updated by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015)

[6] CDL-AD(2016)012, Poland - Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts, adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016)

7 CDL-AD(2016)011,Turkey - Opinion on Law No. 5651 on regulation of publications on the Internet and combating crimes committed by means of such publication ("the Internet Law") adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016)

[8] Budapest, 23.XI.2001. The Republic of Moldova became a Party to the Convention on Cybercrime (ETS 185) on 1 September 2009. The Republic of Moldova also signed the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS 189) on 25 April 2003, but has not ratified it.

[9] Lanzarote**,** 25.X.2007, ratified by the Republic of Moldova on 12.03.2012 and entered into force in respect of the Republic of Moldova on 01.07.2012

[10] See National Action Plan for the implementation of the Association Agreement between the Republic of Moldova and European Union, approved by Government Decision n° 808 of 7 October 2014

(for having breached the proportionality principle).[11] This commitment was also taken into account in the assessment of the draft law.

III. Analysis

a. Article I

17. Article I of the draft law proposes an amendment to Article 7 of the Law on the Service. Existing Article 7 grants the Service a mandate that includes protection against actions that infringe upon the constitutional rights and freedoms of citizens and endanger the security of the state. It also refers to a system of measures, within the power of the Service, aimed at discovering, preventing and counteracting activities which endanger state, public and individual security.

18. The proposed amendment would assign an additional function to the Service at Article 7, sub-paragraph (e), namely to ensure the technical interception of "computer data." As a result, the Service would ensure "*technical interception of computer data and of communications made through electronic communications networks, with the use of special technical means, connected, if necessary, to the network equipment of providers and/or electronic communications services*."

19. This additional wording seems uncontroversial (although broadly framed, the phrase "computer data"[12] seems appropriate in this sub-paragraph context), as long as such computer data interception by the Service can only be carried out for legitimate purposes within the mandate of the Service and subject to adequate protection against abuse of power by the State (see *Iordachi and Others v. Moldova*) in this new area of interception. It is unclear whether the interception system envisaged would enable the Service to obtain communications data without the technical participation of the telecommunications companies who possess the data, i.e. without their knowledge, and without having to show them a duly authorized interception order. Such an interception method involves a greater scope for misuse of power, and as the ECtHR made clear in *Roman Zakharov v. Russia*, must be accompanied by particularly strong safeguards.[13] In any event, the applicable safeguards may be contained elsewhere in the Law on the Service and/or in other Moldovan laws, but they must be specific to the technical interception powers granted to the Service. If not, the proposed amendment, without any further qualification, seems too imprecise since it could encourage the Service to seek to intercept computer data which do not justify its involvement.

20. However, it results from Articles 20 and 21 of the Budapest Convention and its Explanatory Report that only *specified* communications should be the subject of technical interceptions of computer data and of electronic communications. It is therefore suggested to add the term "specified". It is further recommended to add at the end of Article 7 (e) the phrase "ordered according to the law" This reference is meant to ensure that the interception is carried out based on an authorisation by a judge setting forth the legal duration, target and scope of the interception.

21. It must indeed be recalled that the Service does not enjoy unlimited discretion to subject persons within its jurisdiction to technical surveillance. Moreover, interception of computer data by the Service, as ensuing from the new duty that would be assigned to it under Article 7, will

---

[11] CJEU Decision of 8 April 2014 in the joined *cases C-293/12 - Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others - and C-594/12 Kärntner Landesregierung and others.* For more information regarding the situation of data retention in the EU see: Eurojust, Analysis of EU Member States' legal framework and current challenges on data retention, 26 October 2015, available at http://www.statewatch.org/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf

[12] According to the Budapest Convention, the term "computer data" means **"***any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function"*. (Article 1(b))

[13] *Roman Zakharov v. Russia* [GC], no. 47143/06, ECHR 2015, para. 270

almost inevitably result in certain infringements of human rights and fundamental freedoms. It is thus particularly important to read Article 7 in correlation with Article 4 of the Law on the Service, which points out that the Service's operations must ensure observance of human rights and fundamental freedoms (notably to protect against interference with the "private life" of individuals subject to such interception). Also, to ensure respect for proportionality of means, the law should provide, for example, for procedures concerning the transmission of computer data between different authorities, as well as include precise regulations specifying the manner of screening the computer data intelligence obtained through surveillance, the procedures for preserving its integrity and confidentiality and the procedures for storing and destruction of such data.

22. Regarding the scope of the action of the Service and its special investigative activities outside criminal proceedings, under the "security mandate", the Commission and the Directorate recall that "*it is crucial that creating such a mechanism should not undermine the existing safeguards applying to investigations of criminal offences. If the threshold for initiation of a security investigation for a 'security crime' is low, the risk of undermining the ordinary criminal procedure safeguards is particularly strong.*[14]

b. Article II

Article II.2.

23. Article II of the draft law proposes amendments to some provisions of the Criminal Code relating to criminal offences committed involving computer data, including activities carried out via electronic communications systems or other information technologies. The proposed Article II.2 expands Article 178 of the Criminal Code regarding "Violation of the Right to Privacy of Correspondence", and sanctions related thereto, to cover electronic communications. This is to be welcomed as it reflects the commitment to extend the protection of the right to privacy of communication to electronic communications, thereby strengthening the enforcement of Article 8 of the ECHR in practice. This takes into account that the right to respect for one's correspondence sets a high threshold of protection.

24. However, as under Article 8(2) of the ECHR, this protection needs to be made subject to an explicit exception, when such interference constitutes a legal necessary, legitimate and proportionate measure within a democratic society to safeguard national security, public safety or the economic well-being of the country, the protection of health or morals, the protection of the rights and freedoms of others, or for the prevention of disorder or crime. As indicated in the EU e-Privacy Directive,[15] investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system may be a legitimate ground for such interference.

25. For example, an exception for legislative measures providing that, based on such grounds, service providers may retain data for a limited period would be legitimate (s.g. at Article 7 of the Cybercrime Law, discussed below at Article VII.6). Other examples can be found in Articles 132^2, 134^4 and 134^5 of the CCP, pursuant to which service providers may be ordered to engage in acts that could potentially breach correspondence privacy (subject to prior official authorisation). In addition, as discussed in Article III.6 below, a new Article 132^{11} is proposed to be added to the CCP, which would allow for the interception and recording of computer data in relation to the commission of a serious crime. Furthermore, as discussed in Article III.9 below, it is proposed to extend the provisions in Article 134 of the CCP ("Examination and seizure of mail") also to information related to electronic communications. This would enable service providers to, inter alia, open and examine electronic communications following formal notice. As emphasized in the specific sections below, all these measures should be coupled with appropriate legal and procedural safeguards.

[14] See 2014 Joint Opinion, CDL-AD(2014)009, paragraphs 26 and 27 and 55

[15] See EU e-Privacy Directive (2002/58/EC of 12 July 2002) expressly indicating the exceptions to the rule on electronic communications' confidentiality at Article 15(1).

Article II.3.

26. The proposed expansion of Article 208[1] of the Criminal Code regarding "Child Pornography", and sanctions related thereto, to include "*the deliberate obtaining, by means of information technologies or electronic communications systems, of access to*" images of child pornography is to be welcomed. The increase in the maximum prison term permitted in respect of this offence from "1 to 3 years" to "3 to 7 years" is in line with Article 20 paragraph 1 letter f of the Lanzarote Convention, as well as with Article 5 paragraph 6 of Directive 2011/92/UE ["*Production of child pornography shall be punishable by a maximum term of imprisonment of at least 3 years*"].

27. At the same time, higher sanctioning is consistent with the purpose of ensuring applicability of more intrusive procedural powers (search and seizure, interception etc.), as the use of such powers, in line with the requirements of Article 15 of the Budapest Convention, is limited to serious offences. Article 132[1] paragraph 2 of the Criminal Procedure Code indeed includes among the cumulative conditions for having recourse to special investigation measures the existence of "*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*."

28. As regards the offence of "child pornography", it is noted that under Article 9 paragraph 2 b) of the Budapest Convention, the term "child pornography" shall also include pornographic material that visually depicts "*a person appearing to be a minor engaged in sexually explicit conduct*". From the text of the Criminal Code, it is unclear whether such a situation is covered. The provision should be reformulated in such a way as to ensure full implementation of Article 9 of the Budapest Convention. [16]

29. Furthermore, it is recommended that the act of "making available" be also criminalised (in line with article 9 paragraph 1 b) of the Budapest Convention), in order to cover the situation where applications are used for sharing child pornography materials through a computer system, including situations in which the perpetrator has a passive attitude.[17]

30. It is further recommended to complete article 208[1] so as to also ensure protection, as required by article 6 of Directive 2011/92/EU of 13 December 2011, against solicitation of children for sexual purposes by means of information and communication technology, as well as against incitement, aiding and abetting, and attempt to commit the offences listed in this article, in line with article 7 of the EU Directive.

Article II.4.

31. The amendment proposes removal in Article 259 paragraph (1) of the Criminal Code of the need for illegal access to computerised information to have caused "large-scale damage" (although it leaves unchanged the minimum requirement that illegal access must either destroy, deteriorate, block, or copy information, and disrupt computer operations, a computer system or computer network. At the same time in paragraph (2), the causation of "large-scale damages" is inserted as an aggravating circumstance that would justify stronger criminal sanctions (these remain unchanged).

32. These changes seem unobjectionable. As explained by the Government in the Information Note, between 2003 and 2015, out of 407 initiated files, about 94 cybercrime offences could not be investigated because of the requirement for certain offences to produce a damage of at least 45.000 MDL. On the other hand, most of the offences provided by the Budapest Convention do not require a damage to be produced or allow for reservations. Moldova did not make such reservations. Hence, the amendment removing the

[16] The Republic of Moldova did not make use of the possibility of making reservations with respect to Article 9 when depositing the instrument of ratification, thus implementation of all elements of Article 9 is required.
[17] See also Article 5 paragraph 5 of Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.

wording ”and has caused large-scale damage” is consistent with the general approach under Article 2 of the Convention. Illegal access is a basic cybercrime offence and should be broad enough to cover actions that do not lead to damages (see comments below).

33. That being said, the exiting provisions raise issues under Article 2 of the Budapest Convention. First, the approach to criminalise illegal access to *computer data* instead of *computer systems* may raise difficulties in practice in obtaining the evidence (to prove which data was accessed). Second, under the Convention, the intention of Article 2 (illegal access) is to criminalise the mere unauthorized intrusion, which can prevent legitimate users from making use of their systems and data (whether or not this leads to alteration or destruction, which may involve with high costs for reconstruction.) Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery. "Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content related data)[18]. Article 2 allows Parties to attach qualifying elements such as infringing security measures, specific intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another (see Explanatory Report, paragraph 50). However, this option is not available to the Republic of Moldova as no declaration was made upon ratification to this effect. Bearing this in mind, it is important that the Republic of Moldova provide an appropriate scale of penalties for the offence, to take into account that, depending on the circumstances, it can be minor or serious.

34. Notwithstanding this, under the Moldovan law, the criminalization of illegal access is subject to system interference being “*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*”. Therefore, it is likely that a number of acts of unauthorized access, for example in order to obtain computer data, or illegal access not necessarily producing damage, intrusions into protected computers, access by infringing security measures etc. would be considered as legal.

35. It is recommended that the entire Article 259 of the Criminal Code be reformulated so as to ensure, in line with the Budapest Convention, an accurate incrimination of different material facts involving illegal access to computer systems. The term “computerised information” should be replaced with “computer data”, considering that this term is used in other articles of the Criminal Code implementing the Convention. Also, to ensure consistency with the Convention and the Cybercrime Law, the definitions provided by this law (implementing Article 1 of the Convention) should be used.

Article II.5.

36. It is proposed to amend Article 260 of the Criminal Code regarding the production, import, marketing or making available of technical means or software products, to lower existing maximum sanctions. This seems unobjectionable. It is up to the State Party to decide on the sanctions, provided that the penalties are “*effective, proportionate and dissuasive, which include deprivation of liberty*.”[19]

37. Here again, however, the existing provisions of the Criminal Code would deserve comments. Article 6 of the Budapest Convention on misuse of devices requires criminalisation of the production, sale, procurement for use, import, distribution or otherwise

[18] Explanatory Report, paragraphs 44, 46
[19] Article 13 of the Budapest Convention

making available of devices and computer passwords, access codes, or similar data, as well as of the possession of such items. Since no reservation was made in respect to Article 6 by the Republic of Moldova, this article should be duly reflected in the Moldovan law.

Article II.6.

38. It is proposed to amend Article 260^1 on the illegal interception of a computer data transmission by allowing a lower minimum prison term than currently allowed for this offence (replacing “from 2 to 5 years” with “of up to 5 years”). This seems unobjectionable. To avoid any misunderstanding, it is recommended to harmonise the terminology used in this Article (in particular the term “electronic releases”) with that of the Convention (which refers to “electromagnetic emissions”).[20]

Article II.8.

39. The amendment in Article 260^3 paragraph (1) would delete the existing requirement that “large-scale damages” must be caused by the specified activities that could disrupt the functioning of a computer system, but would add a requirement that such activities must be carried out “in an intentional manner and without right”. Also, a lower minimum prison term is introduced (replacing “from 2 to 5 years” with “of up to 5 years”). In paragraph (2), the phrase “especially large-scale damages” would be replaced with the phrase “large-scale damages”, as a factor that would justify stronger criminal sanctions (which remain unchanged).

40. Article 5 of the Budapest Convention on the conduct of “system interference” however includes additional requirements for criminalising system interference. In particular, the hindering must be "serious" in order to give rise to criminal sanction (see paragraph 67 of the Explanatory Report, see also para. 32 above). It is recommended to review the proposed amendment accordingly.

41. With regard to the intentional element, according to the Budapest Convention, the hindering must indeed be "without right" (Explanatory Report paragraph 68). Common operational or commercial practices which are conducted “with right”, such as the testing of the security of a computer system, or its protection, or the reconfiguration of a computer’s operating system, authorised by its owner or operator, should not be criminalised by this article, even if they cause serious hindering.

Article II.11.

42. In paragraph (1) of Article 260^6 regarding “Electronic fraud” it is proposed to delete the existing “large-scale damages”, but to add a requirement that such activities must be carried out in an “intentional and unauthorised” manner. Also, a lower minimum prison term would be permitted than currently allowed for this offence.

43. According to the Budapest Convention (Explanatory Report, paragraph *88),* computer fraud manipulations are criminalised *“if they produce a direct economic or possessory loss of another person's property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person.”* Removing of the (large-scale) “damage” condition for the typical form of this offence is thus not recommended as, otherwise, the incrimination of fraud would be extended to any actions by which the perpetrator aims to obtain a financial gain, but where this result is not achieved and where there is no correlative loss of property for the victim. If there is no damage the act may constitute an attempt. It is recommended that “large scale damage” in paragraph 1 be replaced with “damage” with respect to the typical form of the offence. The proposal to reconsider the scale of sanctions in paragraph (2) is welcome.

[20] Explanatory Report, paragraph 57

44. Finally, it is recommended to review article II of the draft law to ensure that its provisions mirror Articles 8 and 10 of Directive 2013/40/EU of 12 August 2013 on attacks against information systems.

c. Article III

45. Article III of the draft law proposes amendments to the Code of Criminal Procedure. An additional amendment introduced following public consultations proposes to include "electronic communication and traffic data" in Article 126 paragraph (2) CCP providing the grounds for seizing objects or documents. This is to be welcomed as it implies requiring an authorisation of the judge for seizing such "electronic communication and traffic data". Having said this, as noted before, judicial involvement in authorization is only a safeguard if judges are both independent and competent, in law and fact

Article III.1.

46. A new Article 130^1, on "Computer data search and seizure of objects containing computer data", implementing article 19 of the Budapest Convention, is proposed to be added to the CCP. This addition seems globally unobjectionable in light of proposed paragraph 10 imposing that "*the computer search and the seizure of the objects containing computer data shall be carried out in accordance with the provisions of this Code*". In addition, it is important to ensure that the law set out precise provisions regarding the usage and disclosure of any computer data so seized. It should provide, for example, for procedures concerning the transmission of computer data between different authorities, and include precise regulations specifying the manner of screening such data, the procedures for preserving its integrity and confidentiality, and for storing and destroying such data.

47. In response to concerns raised by service providers and NGOs, several new paragraphs have been introduced in the proposed Article 130^1, as follows:

- in paragraph 7 , it is added that "*The seizure of the objects containing computer data, with the exception of those which serve for committing cybercrime offences, can be ordered by motivated ordinance only in exceptional cases (for investigating serious crimes, very serious crimes and exceptionally serious crimes), if for carrying out a computer search or making copies of computer data a long time is required, if the purpose of this measure cannot be achieved another way, and if the measure is necessary and proportional to the restriction of human rights and liberties*."
- in paragraph 8, the maximum period of time for seizing objects containing computer data, with the exception of those which serve for committing cybercrime offences, is limited to the strict time necessary for carrying out the computer search and making copies, which cannot exceed one month.
- in paragraph 10, it is specified that, when the prosecutor orders the termination of the investigation, the copies without any value will be destroyed.
- according to new paragraph 11, the general safeguards provided by the Code for search and seizure are applicable also for computer search.

48. These amendments are welcome. However, notwithstanding the proposed amendments and the reassurance received by the Rapporteurs during the discussions with officials in Chisinau, it is not clear that the proposed text of Article 130^1 prevents the authorities from undertaking a general search of a seized computer, unrelated to the grounds on which the court order was made. Since such searches are an interference with the right to respect for private life, home and correspondence protected under Article 8 ECHR, it is important to provide appropriate safeguards in the legislation both for *when* a search may be authorised and *over the execution* of the search, and that these be strictly limited to purposes that constitute legitimate aims under Art. 8.2 ECHR. It is recommended to introduce wording that limits the searching to the purposes specified in the court order and requires a new court

application before other searching is undertaken. Also, to preserve suspects' or other people's rights, in addition to the alleged crime and subject and the indication to retrieve information/evidence to show the crime, a clause of exclusion of evidence may be inserted in the court order. In addition, enhanced protection should be introduced for categories of especially sensitive information - medical information, legally privileged material and journalistic material. [21]

Article III.2.

49. The amendment in Chapter III of the CCP ("Means of proof and evidentiary procedures") would add a new paragraph to several articles, with the meaning that each of the special investigative measures regulated by these articles could be used in investigating the commission of "*a serious, especially serious, or exceptionally serious crime*",[22] or in relation to a number of listed offences from the Criminal Code. These changes seem unobjectionable with the following caveats.

50. First, in *Iordachi v Moldova,* the ECtHR dealt with the Moldovan "Operational Investigative Activities Act" of 1994, which provided that phone interceptions could be conducted for the investigation of serious, very serious and exceptionally serious offences while the Criminal Code contained a definition of these terms. While the category of crimes liable to give rise to an interception was clearly defined, the Court criticised that '*more than half of the offences provided for in the Criminal Code fall within the category of offences eligible for interception warrants*' (para 44). Second, in respect of some very intrusive special investigative measures likely to result in comprehensive surveillance (such as certain types of GPS surveillance as referenced in Article 134^3 of the CCP), proportionality would only be met when such measures are used in relation to very serious crimes and only after other less intrusive methods had proved less successful.

51. The types of offences that may give rise to an interception warrant - permitting phone tapping - are exhaustively listed in Article 132^8 paragraph (2) of the Criminal Code. However, according to information provided to the Venice Commission, following a first diminution and, subsequently, extensions of this list in 2013 and in 2014, the crimes eligible would represent about one third of the crimes under the Criminal Code and would be rising.

52. From this perspective, recent non-governmental reports (supported by official statistics) regarding the national practice on interception warrants show a situation of great concern and a very disturbing trend in this regard: "*Although back in 2009 the ECtHR noted in the judgment* Iordachi and Others v. Moldova *a too frequent use of phone tapping and a particularly high rate of requests authorised by investigative judges, the official statistics confirm that the situation has not changed significantly. On the opposite, the number of such requests increased significantly. Annually, investigative judges constantly admit about 98% of requests for phone tapping, and this percentage has not changed significantly after the judgment Iordachi and Others was delivered and the legislation was amended […]The statistics […] suggest that the authorisation of phone tapping requests is almost automatic, irrespective of the content of the prosecutors' requests."*[23] A careful examination of the reasons having led to this situation, which raises serious concerns from the perspective of

[21] See, e.g. *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, No. 39315/06), 22 November 2012.

[22] In the state language "*infracţiuni grave, deosebit de grave sau excepţional de grave*"

[23] Legal Resources Centre from Moldova (LRCM), Submission made in accordance with Rule 9.2 of the Rules of the Committee of Ministers, Supervision of execution of the *Iordachi and others v. Moldova* judgment, Sept. 2016 http://crjm.org/wp-content/uploads/2016/09/2016-02-29-LRCM-Submission-Iordachi-and-others-v-Moldova.pdf. The high figures might be partly explicable if these relate to devices monitored, rather than people monitored, on the basis that one person may possess several means of communication. The figures would nonetheless still be high. Besides, this explanation does not clarify why major variations occur from year to year.

fundamental rights, should help the Moldovan authorities determine the most appropriate ways to address this situation, including by reviewing, in the light of the deficiencies shown by the practice, existing legal and procedural safeguards in this field.

Article III.4.

53. It is proposed to amend Article 132^2 of the CCP ("Special investigation measures") at paragraph (1) point 1) regarding the special measures that can be undertaken "in order to uncover and investigate crime" "upon authorisation of the investigating judge". These should also encompass "c^1) interception and recording of computer data". It is also proposed to amend sub-point d) of Article 132^2, paragraph (1) point (1) which refers to "retention, inspection, handing over, search or seizure of mail" to add the words "electronic communications". These changes, intended to introduce interception and recording of computer data and electronic mail in the scope of special investigative measures, seem unobjectionable as long as they take into account the comments made in relation to Article II.2*,* Article III.1, Article III.6 and Article III.12.

Article III.5.

54. It is proposed to include in Article 132^8 paragraph (2) of the CCP (which lists exhaustively the offences in relation to which a warrant for interception and recording of communications may be issued) a reference to Article 174 of the Criminal Code ("Sexual Intercourse with a Person under the Age of 16"). This would enable the interception and recording of communications to find out and store the content of conversations between two or more persons being investigated in respect of this offence, in respect of which (as required by Article 132^8 paragraph (2) CCP) there is data or evidence relating to the commission of this offence. As already indicated, it is important to ensure that these provisions also adequately reflect Article 15 paragraph 3 of Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.

55. This is subject to the proviso (at paragraph (2) that it "*shall exclusively apply to criminal cases having as subject matter criminal investigation or judging persons on which there are data or evidence proving that they have committed offences provided for in [art.174]*". According to paragraph (3) of Article 132^8 of the CCP relating to the categories of persons liable to have their phones tapped, the suspect, accused or persons whose identity was not established may be tapped if there is sufficient data confirming that they contributed to crimes. Yet, paragraph (4) also provides the possibility of authorising phone tapping, at the request of the victim, damaged party, relatives, his/her family members and witness, if there is imminent danger for his/her life, health or other fundamental rights, if it is necessary to prevent a crime or if there is a clear risk of irreparable loss or distortion of evidence.

56. The caveat that there must be sufficient data confirming that those to be monitored contributed to crimes should alleviate the concern that the circle of surveillance is too wide, as long as it is upheld to a high standard of proof in this context.[24]

[24] In *Iordachi v Moldova*, the ECtHR noted that the language of the law, which prescribed that "suspects, defendants or other persons involved in a crime" could be intercepted, did not indicate with sufficient clarity, which category of persons might be affected by phone interceptions. In particular, the Court pointed out that there was no definition of the term "*other persons involved in a criminal offence*'' (too large a category) (para 44). By way of contrast, the ECtHR found the German law which regulate phone interceptions by German intelligence agencies, to be compliant with the requirements of Article 8 ECHR (*Klass v Germany*, paragraph 51 read with paragraph 17). Pursuant to this law, persons who could be targeted by interceptions were "*the suspect or such other persons who are, on the basis of clear facts, to be presumed to receive or forward communications intended for the suspect or emanating from him or whose telephone the suspect is to be presumed to use*".

Article III.6.

57. A new Article 132[11] ("Interception and recording of computer data") is proposed to be added to the CCP. This amendment would allow for the interception and recording of computer data consisting in "*the use of technical measures 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 communication transmitted through a computer system, and the storage of information obtained following interception on a technical medium*". This power would only be available in relation to investigating the commission of "a serious, especially serious, or exceptionally serious crime", or in relation to a number of listed offences.

58. First, a clear distinction must be made between intercepting and recording of computer data (used in the title of the proposed Article 132[11]) on the one hand, and intercepting and recording traffic data in real time (to which is also made reference in the text of the article), on the other hand (see Budapest Convention, article 19[25]). Also, it would be advisable to treat these measures separately, in distinct legislative provisions (see article 19 and article 20 of the Budapest Convention) and to provide clear definitions of these measures, or to make reference to the definition of traffic data stated by the Cybercrime Law.

59. Second, as mentioned above (see, in particular, the comments made at Article II.2, Article III.1, Article III.4, Article III.5 and Article III.12), the law should provide for procedural safeguards around the collection and use of computer data in a criminal investigation. Examples include setting out precise rules regarding the transmission of computer data between different authorities, as well as specifying the manner of screening the intelligence obtained through surveillance, the procedures for preserving its integrity and confidentiality and the procedures for storing and destruction of such data.

Article III.8.

60. It is proposed to add the words "and of electronic communications" to the title of Article 133 of the CCP ("The retention, inspection, delivery, search or seizure of mail"), as well as to all references to "mail" throughout Article 133. These amendments seem uncontroversial, as long as such electronic communications interception duties by the Service can only be carried out for legitimate purposes within the mandate of the Service as complemented by the draft Law, and subject to adequate protection against abuse of power by the State, as set out in *Iordachi and Others v. Moldova*, in this similar field of interception (see comments in respect of Article I).

Article III.9.

61. It is proposed to add a new paragraph (4) to Article 134 of the CCP (which contains procedural guarantees[26] for the "[e]xamination and seizure of mail") indicating that the provisions of this article shall be enforced correspondingly in the case of information related to electronic communications, too". Comments made in respect of Article II.2 and Article III.8 above are applicable.

Article III.10.

62. It is proposed to amend Article 134[2] of the CCP (on monitoring or control of financial transactions and access to financial information) by enlarging, with some relevant offences,

[25] "Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a: a - computer system or part of it and computer data stored therein; and b : a computer-data storage medium in which computer data may be stored in its territory" (article 19.1).

[26] In terms of information regarding the relevant judge ordinance, seizure of the concerned mail, minutes to be taken on each mail examination or seizure, the obligation of keeping the secrecy of correspondence.

the list of crimes for which "*monitoring or control of financial transactions and access to financial information shall be ordered*", when criminal investigation has been initiated.

63. This change seem unobjectionable on the assumption that these offences are extremely serious, bearing in mind the comments made in the 2014 Joint Opinion: "*[f]inancial information relating to individuals is likely to contain some personal data and, depending on the transactions concerned, may be connected to aspects of private life. The storing and the release of such information will amount to an interference with the right to respect for private life as guaranteed by Article 8 ECHR. […] to allow the Service access to all financial records (as opposed to suspicious transaction notifications, as regards money laundering, which it is permissible to provide for) is a system which invites abuse. Nor is it proportional*." It is noted that some of the offences to be added to the existing list in Article 134[2] of the CCP are drafted so broadly that the trigger for launching an investigation into their commission may be low (see, e.g. "violation of copyright and related rights"). It is noted in this respect that the Budapest Convention (Article 10.1) only requires to establish as criminal offences the infringement of copyright, as defined under domestic law, "where such acts are committed wilfully, on a commercial scale and by means of a computer system".

Article III.12.

64. It is proposed to add to Article 305 of the CCP ("Procedure for examining actions regarding the authorization of the conduction of criminal prosecution actions, operational investigative actions and the application of the coercive procedural measures") at paragraph (3), the phrase ", upon interception and recording of computer data". A formal request to engage in such interception and recording of computer data in a particular case would therefore have to be *examined* by the investigative judge immediately, and no later than 4 hours after the request was received. (See Article III.4)

65. Bearing in mind the degree of intrusion a special investigative measure can entail for the right to privacy, it seems vital that the judge be able to request whatever supporting documentation s/he considers necessary and to question the participants in the proceedings. Yet, article 305 of the CCP does not state how long the judge has to consider the request or whether an answer has to be given within 4 hours. According to paragraph (4) of article 305, "*[w]ithin the set timeframe the investigative judge shall open the hearing, announce the motion to be examined and verify the authority of the participants in the proceeding*". Paragraph (7) adds that following the control over sufficiency of the motion, the investigative judge shall authorize or reject the motion. Both provisions lack indication on the actual deadline provided to the judge for giving an answer. Should 4 hours (rather than 24 hours) be the judicial turnaround to authorise the interception and recording of computer data, it would be highly onerous (see also related comments in the 2014 Joint Opinion, paragraph 44).

d. Article IV

66. Article IV.1 adds a new point e[1]) to Article 17 ("Professional obligations of the doctor") of the Law on the medical profession, which would oblige doctors to transmit to law enforcement bodies "*any information, they have learnt about in the exercise of their job duties, regarding abuse cases and violence, including sexual ones, directed towards children."*

67. Any sharing of information must comply with laws (as well as any healthcare-specific professional codes in the Republic of Moldova) relating to confidentiality, data protection and human rights. Medical information is especially sensitive personal information, protected under Art 8 ECHR.[27] Patient confidentiality - the presumption that all information provided by

[27] See *Z v. Finland*. (9/1996/627/811), Judgment of 25 February 1997; *Peck v. United Kingdom, Application no. 44647/98, Judgment of 28 January 2003.*

a patient to their medical professional will be treated as confidential and not shared with a third party - is critical to any medical professionals' legal and moral obligations. This is confirmed by current point e) of Article 17, as well as by article 13 (on the professional secret) of the Law on the medical profession.

68. It is noted that, while Article 12(1) of the Lanzarote Convention refers to the "possibility" of reporting, the Moldovan law would impose an obligation on doctors to report. In the case of evidence of child victims of violence or sexual abuse, mandatory reporting as required by the proposed provision is clearly justified. However, the obligation is not confined to medical professionals "in contact with children" but could be triggered by contact with adult family members or by information originated at different potential sources. Moreover, the reasonable suspicion criterion has been omitted and replaced with a reference to "any information". This could, for example, be taken to impose a duty on doctors to transmit any allegation of abuse, even if unsupported by other medical indicators. Finally, the amendment appears to impose duties of disclosure beyond the Lanzarote Convention, concerning child abuse and violence generally, whether or not it involves sexual exploitation.

69. It is noted in this connection that the disclosure of information about violence is already addressed in Article 13 point c^1) of the Law on the medical profession, (presumably implementing the requirements of the UN Convention against Torture[28] and the UN Convention of the Convention on the Rights of the Child[29]), and therefore the wider reference to violence in the proposed point e^1) may be seen as redundant.

70. It is recommended that the wording of the proposed text be reconsidered in the light of the Lanzarote Convention grounds, and better correlated with other related provisions in the Law on the medical profession.

e. Article VI

Article VI.1.

71. Article VI of the draft law proposes amendments to the Contravention Code. A first amendment aims at expanding the offence in Article 90 ("Producing, selling, distributing or storing pornographic products") to cover the deliberate accessing of pornographic products in public places. This proposal raises issues of foreseeability and proportionality. First, there does not seem to be any definition of pornographic products in the text (nor of "public paces"). If such a definition is provided by other laws, it would be advisable to introduce a reference to the concerned provisions. Besides, sanctioning all types of access to pornographic products would arguably amount to sanctioning legitimate activities, such as research activities. The proposed amendment and article 90 of the Contravention Code should be revised accordingly.

Article VI.2.

72. A new Article 247^1 is proposed to be added in Chapter XIV of the Contravention Code setting out offences "in the field of electronic communications, mailings and information technologies". This new Article describes infringements that may be committed by providers of electronic communication services, together with the corresponding sanctions.

[28] UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, adopted in 1984 and entered into force in 1987.
[29] See UN Convention on the Rights of the Child, adopted in 1989 and entered into force in 1990 (art.19)

73. These proposed new offences are: a) failure to keep user records; b) failure to report to competent authorities specified incidents "*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 with an authority request regarding data preservation; d) failure to submit user or traffic information following a request "made under the terms of procedural legislation"; e) failure to enforce certain security measures; f) failure to preserve traffic data "*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 stop, 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.*"

74. Most of the obligations that must be met by service providers have been introduced through Article 7 of the Cybercrime Law. The proposed article establishes the offences for non-compliance with those obligations; at the same time, new obligations would now be added, such as blocking certain types of content, in paragraph g) of proposed article 247[1].

75. As a general observation, it is noted that new Article 247[1] seems to mix civil/administrative transgression with procedural non-compliance, which is likely to create confusion. Parts of this article, which is clearly aimed at implementing article 18 of the Budapest Convention, should rather be included, in line with the standards of the Budapest Convention, in the Code of Criminal Procedure. Accordingly, the above quoted letters c), d) f) should be procedural infringements and not contraventions. Also, since Article 18.1b referring to the obligation of service providers to provide (upon order by the competent authorities) subscriber information in their possession or control is now being discussed in the Budapest Convention Committee, the Moldovan authorities may want to consider the outcome of these discussions in future amendments.

76. In addition, clear distinction should be made, both in the Moldovan legislation and in the application of these measures, in line with the clarifications made in the framework of the Budapest Convention,[30] between the *preservation of data* (that is, freezing relevant data, including content data in order to allow time for obtaining a court order for the production or seizure of data), and *data retention* obligations, which stand for a mandatory continued storage of information (normally traffic data) for a certain time by the service provider[31].

77. From this perspective, it is positive that, through an additional amendment a new article is added to the draft law (Art. IX - Final and transitory provisions), which postpones the entering into force of Article VI.2 by 6 months in order to allow the Government to draft, consult and approve the list of categories of data to be retained, contained in this article and the service providers to adapt their systems to the new requirements.[32]

78. In this connection, during the exchanges held in Chisinau, a number of concerns have been raised with regard to the draft law, by representatives of civil society organisations and of the National Association of IT Companies of the Republic of Moldova. These are related

[30] See, for further clarification, the Explanatory Report of the Budapest Convention (paragraphs 149-162), and .*Assessment Report on the Implementation of the preservation provisions of the Budapest Convention on Cybercrime* adopted by the T-CY at its 8th Plenary (5-6 December 2012).

[31] deadlines for the two measures are provided by article 7 of the Law on preventing and combating cybercrime : 120 days for preservation of data, and 180 days for data retention

[32] In two months from the date of publication of the law, the Ministry of Internal Affairs will have to submit to the Government a list of categories of data to be retained by service providers.

to: overlapping of norms regulating the providers' obligations across different laws; lack of a clear definition of the categories of data to be retained; lack of clear specification of the authorities entitled to have access to the retained data; excessive although incomplete norms regarding access to data; contradictory norms on the duration of retention of data; obligation to retain the content data or obligation that are impossible to be executed; liability for breach of the legislation by third parties; unclear and expensive obligation to ensure the security of infrastructure and incidents reporting; excessive but incomplete norms on ceasing/blocking access to web pages (see further below, the comments on Article VII 6). In the view of the Venice Commission and the Directorate, it is vital for the successful implementation of the government's policy of preventing and combating cybercrime, to provide clarity on the various aspects raised, including by taking into account the observations provided in the present Opinion.

f. Article VII

79. Article VII of the draft law proposes amendments to the Cybercrime Law. Following the ratification of the Cybercrime Convention in 2009, and starting with the adoption of the Cybercrime Law in February 2009, several rounds of amendments of relevant Moldovan legislation (including the Criminal Code and Criminal Procedural Code) have been adopted to implement its requirements. However, these legislative measures have been criticised as having many flaws resulting in implementation problems (see above concerns expressed by the civil society). The current amendments are aimed at addressing such criticism.

Article VII.1.

80. It is proposed to amend Article 2 of the Cybercrime Law ("Main concepts") with new definitions regarding: "critical infrastructure"; "owner/operator/administrator of the critical infrastructure"; "preservation of data"; "computer data security"; "computer security incident"; and "cyber criminality".

81. The definition of "critical infrastructure"[33] follows closely *Council Directive 2008/114/EC of 8.12.2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, which is a positive step. It is also positive that, through an additional amendment, it is now proposed to complete the definition of "traffic data" with the following wording: "*traffic data does not include content data that represents or discloses the content of electronic communications, including information consulted by using an electronic communication network*". This would respond, *inter alia,* to situations encountered in practice, when some investigative bodies request URL addresses of web pages accessed by users considering that this is not content data, but traffic data.

82. As to the proposed notion of "cyber criminality", it is arguable whether such a broad definition[34] should be transposed into the criminal law. Neither the Budapest Convention nor relevant EU Directive[35] provide this term. For example, it would be difficult to maintain criminal justice statistics if any ordinary crime involving computer data or a computer system were considered to constitute cybercrime. It is recommended to reconsider this notion.

---

[33] "*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;*

[34] *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*

[35] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Article VII.5.

83. A new Article 6^1 is proposed to be added to the Cybercrime Law, entitled "Obligations of critical computer infrastructures". According to the initially proposed paragraph d) of Article 6^1, in order to prevent cyber criminality, owners and operators of critical computer infrastructures were obliged to "*communicate immediately to the competent authorities, no later than **24 hours** [emphasis added] from the moment of detection, information about the illegal access to their own computer data system, attempts to introduce illegal programmes, the violation […] 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."* Following public consultations, some amendments to this text have been proposed by the Government, amendments which generally seem to go in the right direction.

84. First, the notification period has been extended to 72 hours, which appears to be in line with the corresponding EU regulations.[36] Second, a number of criteria defining "incidents with a significant impact" are now provided in an additional paragraph 2 of Article 6^1. These include: the number of users and the geographical area affected; the impact on other owners/operators of critical computer infrastructures; the impact (in terms of gravity and duration) on vital economic and social function or public security; the availability of alternative ways to provide the concerned computer services. Third, a further paragraph has been inserted into new Article 6^1 stipulating that the authorities competent for receiving and processing information communicated by owners/operators shall be set by governmental decision. While this addition aims to respond to concerns expressed by service providers, one may wonder whether it would not be advisable to specify these authorities in the law itself, in view of the sensitivity of the task assigned to them.

Article VII.6.

85. Several points of amendment have been proposed in respect of Article 7 of the Cybercrime Law regulating the obligations of service providers in relation to issues such as preservation, retention and disclosure of information.

86. In paragraph (1) point c), it is proposed that the existing obligation upon service providers to ensure "immediate" preservation of computer data or traffic information following an authority request (where there is a danger of its destruction of alteration), be changed to "rapid" preservation. This is a welcome change, aiming at harmonizing the Moldovan law with Article 16 of Budapest Convention (which speaks of "expedited" or "expeditious" preservation). At the same time, the increase, from 120 calendar days in the law in force to 180 calendar days, of the period of time for which data must be preserved, goes against the requirement of the Convention that "the period of time should be as long as necessary, up to a maximum of 90 days". This provision should be revised, taking into account that, although the Convention allows (Article 16 of the Convention) subsequent renewal of a discloser order, it establishes, in line with the principle of proportionality, a shorter period for data preservation. Under Article 132^4 of the CCP of the Republic of Moldova, "[t]he special investigative measure shall be decided for a 30-day period, with the possibility of a 6-month

[36] By way of comparison, the EU NIS Directive (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union) provides for an obligation to notify without undue delay, whereas the General Data Protection Regulation - GDPR (Regulation (EU) 2016/679) opted for a 72 hours delay with an exception when such notification cannot be achieved within 72 hours.

extension for justified reasons, unless otherwise is provided by this Code. Each extension of the period for the special investigative means cannot exceed 30 days. […]".

87. Under revised point d), service providers would be obliged to submit to the competent authorities, in addition to the existing requirement to submit user-related data, data "relating to information traffic".. It would be important to specify the link between revised point d) and the proposed new CCP Article 132[11] discussed in Article III.6 above (which would allow for the interception, recording and storage, in real time, of data referring to the cyber traffic and/or data related to contents associated to the given communication transmitted through a computer system).

88. In paragraph (1) point f), it is proposed to change the existing obligation imposing service providers to keep traffic data (for the identification of service providers, and users, and the channel through which communications have been sent) for a period of 180 calendar days. Traffic data recorded in fixed and mobile telephone networks would be kept for one year, while internet traffic/telephony traffic data would be kept for six months. The existing obligation upon service providers to ensure the "monitoring" and "surveillance" of traffic data would be deleted, which is a positive amendment.

89. The extension of the current data retention period should however be justified, together (in particular) with the proportionality of the one-year retention period to be set for the retention of traffic data recorded in fixed and mobile telephone networks. To note, while different data retention periods for different categories of data are justifiable (on the basis of their possible usefulness for the legitimate purposes pursued), each data retention period must be based on "objective criteria" in order to ensure that it is limited to what is strictly necessary[37]. The more data that is retained, the more data can be leaked if the operator's system is penetrated, or its personal is corrupted. At the same time, it is true that, in order to assess a data retention scheme, it is essential to take into account all available safeguards and in particular the modalities of the supervision and of the access regime in place.

Internet Blocking

90. The inclusion of a new point h) in paragraph (1) of Article 7 of the Cybercrime Law, dealing with the obligations imposed on providers in terms of Internet access blocking, has prompted criticism both on the part of the public and service providers. Under new point h), in the first version of the draft law, service providers would be required "*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*" (emphasis added). At the same time, the draft law modifies Article 247[1] of the Contravention Code imposing a fine upon service providers for failure to fulfil this obligation (see under Article VI).

91. There is no international instrument that requires service providers to stop access to child pornography and other illegal content. In its Recommendation to member states on measures to promote respect for freedom of expression and information with regard to Internet (CM/Rec(2008)6), the Council of Europe Committee of Ministers stated, *inter alia*, that states should refrain from filtering Internet content for reasons other than those laid down in Article 10, paragraph 2 ECHR, as interpreted by the ECtHR, and should guarantee

[37] See comments by the Court of Justice of the EU in the joined cases C-293/12 - *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others* - and C-594/12 *Kärntner Landesregierung and others*, where a mandatory data retention period of between six to 24 months was considered to be disproportionate.

that nationwide general blocking or filtering measures are only introduced if the conditions of Article 10, paragraph 2 ECHR are fulfilled. Notably, in the Recommendation, the interests of minors are taken into account, through the possible implementation of filters in certain places, such as schools or libraries. The Recommendation further states that "*[s]uch action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights*."

92. The Committee of Ministers also stresses, in its Recommendation CM/Rec(2016)5 on Internet Freedom, that "*before restrictive measures to Internet access are applied, a court or independent administrative authority determines that disconnection from the Internet is the least restrictive measure for achieving the legitimate aim*".

93. The ECtHR, as indicated in the Venice Commission 2016 Opinion on the Internet Law of Turkey,[38] has a relatively rich case-law relevant in the Internet context, concerning in particular restrictions imposed on freedom of expression on the Internet, data-protection and retention issues relevant for the Internet under Article 8 ECHR, Internet and intellectual property, obligation of States to combat violence and other criminal or unlawful activities, and access to information and the Internet under Article 10 ECHR.

94. Article 10 includes *the right to receive and impart information.* and the Internet certainly falls within the scope of Article 10. In the case of *Times Newspapers Ltd v. the United Kingdom,* the ECtHR, applying the general principles developed in relation to Article 10 ECHR to cases concerning *online* publication, stressed that: "*In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general […]*"[39]The Court also explicitly stated that blocking Internet access may be "*in direct conflict with the actual wording of paragraph 1 of Article 10 of the Convention, according to which the rights set forth in that Article are secured 'regardless of frontiers.'*"[40]

95. Under the terms of paragraph 2 of Article 10, the exercise of the freedom to receive and impart information may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society in the pursuit of a legitimate aim. In the context of the freedom of the press, the Court has frequently underlined that not only does the press have the task of imparting information and ideas of public interest, the public also has the right to receive them. Therefore, particularly strong reasons and safeguards must be provided for limiting access by the public to Internet, a measure which, by rendering large quantities of information inaccessible, substantially restricts the rights of Internet users and is likely to have significant collateral effects.

96. In the view of the Court, prior restraints such as Internet blocking orders "*are not necessarily incompatible with the Convention as a matter of principle. However, a legal framework is required, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power […]. In that regard, the judicial review of such a measure, based on a weighing-up of the competing interests at stake and designed to strike a balance between them, is inconceivable without a framework establishing precise and specific rules regarding the application of preventive restrictions on freedom of expression […].*"[41]

---

[38] See CDL-AD(2016)016, Turkey - Opinion on Law No. 5651 on regulation of publications on the Internet and combating crimes committed by means of such publication ("the Internet Law") adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016), paragraph 36.

[39] In *Times Newspapers Ltd v. the United Kingdom,* Application Nos. 3002/03 and 23676/03, 10 March 2009, para. 27

[40] *Ahmet Yıldırım v. Turkey*, Application No 3111/10, Judgment 18.12.2012, paragraph 67

[41] *Idem*, paragraph 64

97. Also, within the European Union framework, under Article 25 of Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography,[42] EU Member States have the possibility to *"take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory."* However, Article 25 adds that these measures "*must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress."*

98. In view of the above background, it is positively noted that, through an additional amendment, the Moldovan authorities decided to modify the text of point h) of Article 7 of the draft law, so as to ensure that providers will only be obliged to block access to the webpage containing harmful content instead of, as was the case in the first version of the text, blocking access *to all IP addresses on which the concerned webpage is located*.

99. Moreover, a new paragraph 3 was added to Article 7, indicating that the blocking of the access to webpages, as foreseen in paragraph (1) point h), shall be ordered by court decision, in the framework of a criminal case, i.e. when the service provider has not removed the harmful information from the webpage hosted/or being under his control, at the request of the law enforcement authority, or when the determination of the contact details of the service provider was not possible. In addition, this new paragraph specifies that "the interruption of access to websites containing child pornography, promoting sexual abuse or sexual exploitation of children that are not hosted by the provider concerned, shall be ordered by the law enforcement authority in accordance with the List drawn up by the International Organization of Criminal Police (INTERPOL "Worst of" List), which should be made available to the service provider.

100.Finally, the Moldovan authorities have now proposed to delete from the list of grounds/criteria for access blocking the web pages "containing or disseminating instructions on how to commit crimes", which is also a commendable proposal.

101.Also, the revised draft article 7 would include an additional paragraph 1^1 stipulating that the category of data to be retained by service providers shall be established by the Government.

102. According to the accompanying Information Note to the new amendments, the aim was to ensure that the law also establishes the conditions for implementing the blocking obligation, as a way to avoid imposing on providers obligations which would be in breach both with the fundamental rights principles and with more specific standards in the field. The Information Note further stresses the need to set out a procedure, in the current law or elsewhere in the Moldovan legislation, determining the following: which authority is empowered to identify and assess contents according to the criteria set out in point h) and to ask for their deletion or the blocking of the access to the concerned webpage; the evaluation procedure and the modality for communicating the decision to the service provider, as well as the legal remedies available against the deletion/blocking decision. This is a welcome approach, also in line with Directive 2000/31/EC[43]**,** stating that States shall not impose a general obligation on providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

[42] Directive 2011/92/EU, p. 1–14.
[43] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Article 15.1

103.More generally, the proposed amendments and further envisaged changes to the initial text of the draft law reflect the Moldovan authorities' effort to improve the rules for blocking measures in terms of precision and clarity. Nevertheless, additional steps are needed to bring them fully in line with the applicable standards.

104.Although the grounds for blocking under Article VII.6 would in principle constitute legitimate aims under Art. 10. 2 ECHR, there is scope for improvement as regards their formulation, which for some of the offences listed may appear overly broad.

105.Also, while the choice to adopt a two-step process and resort to blocking orders only after having requested hosting providers to take-down the content is to be welcomed, a more detailed description of these two steps and their interplay would help to enhance the clarity of the legal basis.

106.Furthermore, while Article VII.6 in its latest version requires the blocking of web pages only (without references to IP addresses, as was the case in the first version), the text remains vague and it is not sure whether judges would make sure that service providers do not simply impede access to content at the domain level. Blocking access at the domain level raises serious concerns in terms of reasonableness and thereby necessity and proportionality in the context of the applicability of both Articles 8 and 10 of the ECHR.[44]

107.In addition, there is no possibility for Internet users to oppose blocking orders. It is recalled that Recommendation CM/Rec(2008)6 makes it clear that the provision of *"effective and readily accessible means of recourse and remedy, including suspension of filters,"* is crucial to cater for *"cases where users and/or authors of content claim that content has been blocked unreasonably."*

108.Finally, the reasonableness/proportionality of the filtering or blocking access should also require an assessment of the costs of the technologies to be used when implementation is required by law. Recommendation (CM/Rec(2008)6) expressly encourages States to "*ensure that all filters are assessed both before and during their implementation to ensure that the effects of the filtering are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unreasonable blocking of content*."

109.It is recommended that the provisions regulating access blocking be revised and further elaborated in the light of the above observations.

g. Article IX

110.As already indicated, under a new article IX - Final and transitory provisions - it is proposed to postpone the entering into force of article VI.2 by 6 months in order to enable the Government to elaborate further the list of obligations/contraventions contained in this article, in consultation with service providers. Furthermore, the Ministry of Internal Affairs will have to draft and submit to the Government a list of categories of data to be retained by service providers within a two-month deadline. This amendment is most welcome.

IV. Conclusions

111.Draft law N°161 and the additional draft amendments proposed following public consultations, aim at improving the Moldovan legal framework for the implementation of the country's policy in the area of information security protection and prevention and fight against cybercrime, as well as against on-line sexual exploitation and abuse of children, in

[44] See *Yildirim v. Turkey* and in *Cengiz and Others v. Turkey*, where the ECtHR condemned the blocking at the domain level ordered by the Turkish criminal court.

line with the commitments undertaken by the Republic of Moldova under the applicable European instruments.

112.Further legislative amendments are pending - which are outside the scope of the present Opinion - concerning the legal framework pertaining to special investigation activities, as well as to the mandate, organization and operation of the Moldovan Security and Intelligence Service. These reportedly include rules related to the “security mandate” established as a new mechanism for security investigations enabling the Service to perform special investigative measures outside of the framework of a criminal investigation.

113.Provided that the observations made by the Venice Commission and the Directorate in the present Opinion are properly taken into account, and that the provisions of the current draft law are adequately correlated with relevant provisions which are the subject of other pending legislative processes, the proposed amendments will bring improvement to the Moldovan legislation and contribute to its further alignment to the applicable European standards.

114.The Venice Commission and the Directorate have examined the draft law and have identified the main issues which need to be addressed by the authorities of the Republic of Moldova in order for the draft law to meet those standards:

- ensure, in the framework of the interception of computer data, as well as in relation to computer data search and seizure of objects containing computer data, respect for the proportionality of means, by providing, in the law, for: appropriate safeguards both for the grounds, the procedure and the deadlines for authorizing a search, and the execution of the search; procedures concerning the transmission of computer data between different authorities; precise rules specifying the manner of screening the data obtained through surveillance, procedures for preserving its integrity and confidentiality and for the storing and destruction of such data;

- provide increased clarity with regard to data retention obligations (categories of data to be retained, deadlines, authorities entitled to receive and process data, etc.) and ensure full respect of the principle of proportionality in this area, in line with relevant European norms and case-law;

- revise the provisions on the offence of "child pornography" in the Criminal Code so as to bring them fully in line with Article 9 of the Budapest Convention; reformulate, in line with the Lanzarote Convention, the provisions relating to the obligation imposed on doctors to report in the case of evidence of child victims of sexual abuse;

- reformulate Article 259 of the Criminal Code so as to ensure, in line with the Budapest Convention, an accurate incrimination of different material facts involving illegal access to computer systems;

- revise and specify further the framework regulating Internet access blocking, to bring it fully in conformity with fundamental rights principles and safeguards, as enshrined in the ECHR and relevant case law, and more specific standards and regulations in the field.

115.To avoid confusion in the interpretation and application of the law, it will be essential to ensure terminology consistency throughout the law and make use of the definitions provided by the Cybercrime Law implementing Article 1 of the Budapest Convention. Furthermore, clarity is needed with regard to the concepts used in the law, in line with the Budapest Convention (e.g. interception and recording of computer data//intercepting and recording traffic data in real time; preservation of data//data retention).

116.The Council of Europe is supporting the Republic of Moldova through regional capacity building projects. Two joint projects with the European Union are currently underway, namely, Cybercrime@EAP II on international cooperation and Cybercrime@EAP III on public/private cooperation on cybercrime and electronic evidence. Both projects include the option of support to criminal law reform. The authorities of Moldova are encouraged to draw on Council of Europe capacity building projects with a view to further strengthening its legal framework on cybercrime and electronic evidence.

117.The Venice Commission and the Directorate are ready to provide any further assistance to the Moldovan authorities, should they request it.