LRCM | LEGAL RESOURCES CENTRE FROM MOLDOVA

33 Ştiusev str., MD-2001 Chişinău, Republic of Moldova; tel: +(373) 22 843 601; fax: +(373) 22 843 602; web: www.crjm.org

Opinion on the Draft Law no. 161 on Amendments and Supplements to Certain Legislative Acts ("Big Brother" Law)[1]

Date: 23 November 2016

Contents

Summary:

Draft Law no. 161 on Amendments and Supplements to Certain Legislative Acts (called „Big Brother" Law) raises several general and specific issues relating to the way these provisions could be applied, as well as those that

[1] This opinion has been prepared by Bogdan Manolea in collaboration with the Legal Resources Centre from Moldova (LRCM) under the project „Promoting Effective Judicial Accountability Mechanisms in Moldova" implemented by LRCM with the financial support of the Justice Programme of Soros Foundation-Moldova. The opinions expressed in this document belong exclusively to the author and do not necessarily reflect the position of the funding institution.

The Legal Resources Centre from Moldova (LRCM) is a non-profit non-governmental organization based in Chisinau, Republic of Moldova. LRCM strives to ensure qualitative, prompt and transparent delivery of justice. In achieving these aims, LRCM combines policy research and advocacy in an independent and non-partisan manner. LRCM was involved in drafting of several policy documents and laws.

Bogdan Manolea is a lawyer specializing in information technology law for over 15 years, his domain of interest is how technology intervenes with human rights as well as any other domains involving law, Internet and civic attitude. Bogdan is the owner of the webpage Internet Laws - legi-internet.ro, which since 2001 presents the key developments in the domain of information technology law, and the Executive Director of the Association for Technology and Internet - ApTI. Bogdan is the author of over 150 presentations and articles on topics related to Law and Information Technology that were presented at national and international events.

could affect fundamental rights, and, in particular, the right to privacy, without being justified as necessary in a democratic society in line with the practice of the European Court of Human Rights (ECtHR).

Thus, while in the European Union (EU) the limitation of *mass surveillance* measures is discussed in the context of the European Court of Justice (ECJ)[2] and four EU member states constitutional courts[3] decisions relating to the laws on retaining traffic data, it is ominous that in the Republic of Moldova new laws on broadening the obligations to retain traffic data are being proposed without any comprehensive analysis of the need for interference with the fundamental rights.

Moreover, introduction of some amendments from various domains and areas of interest to multiple normative acts - some of which may be reasonably grounded, others certainly questionable and affecting fundamental rights - raises legitimate questions about the need for each particular measure and extent to which such need is grounded.

For instance, the actual implementation of the proposal to block access to "all IP addresses that host webpages (...) containing information that urge to hatred or ethnic, racial or religious discrimination, to hostility or violence" would lead directly to blocking Facebook, Youtube or Twitter in the Republic of Moldova, although we are sure that this was not what the legislator wanted.

Our particular recommendations for each article are detailed below, still, they would generally refer to:

- rejection of the proposed articles that would imply mass surveillance measures (such as those related to data retention, in particular Art. VI, p. 2 of the draft law no. 161 (amendment of Art. 247[1] of the Contravention Code); Art. VII, p. 6 (amendments to art. 7 of Law no. 20 on Preventing and Combating Cybercrimes, particularly problematic ones being paragraph (1) letter a), c), f), h));
- detailed examination of legislation that extends the limitation of fundamental rights, including a study of impact on human rights based on the ECtHR case law and expertise;
- waiving the obligations to "stop" access to web pages. Blocking of web pages by ISP represents an interference with the normal Internet traffic between users and websites, which raises violation of freedom of expression and the right to privacy by means of creating a layer of censorship. It is important to understand the difference between:
    - stopping access / blocking - when the content remains on the Internet, visible to most users, but hidden for the users from the Republic of Moldova who are subject to blocking.
    - deletion of contents from the Internet – when the illegal content cannot be anymore found online.

We believe that the only right solution can be deleting any unlawful content, coupled with a criminal

---

[2] CJEU decision in C-362/14 Maximillian Schrems/Data Protection Commissioner case http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117ro.pdf and CJEU decision as of 8 April 2014 in Joined Cases C-293-12 and C-594-12 *Digital Rights Ireland* *http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=RO*.

[3] Decision 1258/2009 by the Constitutional Court of Romania- http://www.legi-internet.ro/jurisprudenta-it-romania/decizii-it/decizia-curtii-constitutionale-referitoare-la-legea-pentru-pastrarea-datelor-de-trafic-298-2008.html; Decision by the Constitutional Court of Slovakia (2014): http://fra.europa.eu/en/caselaw-reference/slovakia-constitutional-court-slovak-republic-pl-us-102014-78; Decision by the Constitutional Court of the Czech Republic (2011): http://www.usoud.cz/en/decisions/20110322-pl-us-2410-data-retention-in-telecommunications-services/; Decision by the Constitutional Court of Germany (2010): http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.

investigation with the view to identify offenders who took the illegal child pictures and / or published them online;

- clarification of terminology, preserving technological neutrality in wording and clear explanation of terms depending on technology used;
- encouraging voluntary collaboration in reporting cybercrimes.

Draft law analysis and particular recommendations:

The draft law on Amendments and Supplements to Certain Legislative Acts, adopted by the Government on 11 April 2016, registered in the Parliament on 13 April 2016 under no. 161 (*hereinafter referred to as „draft law no. 161"*) raises several general and specific problems regarding the way these provisions could be applied, as well as those that could affect fundamental rights, and, in particular, the right to privacy, without being justified as necessary in a democratic society in line with the practice of the European Court of Human Rights (ECtHR).

For this purpose, we present seven general high priority issues to be considered under this normative act followed by a series of major specific issues on the publicly available text.

A. General issues

Need for any interference with fundamental rights must be proved

First of all, we consider that any normative act which inherently brings about limitations of fundamental rights must be accompanied by a thorough impact analysis. Thus, **any interference with the exercise of a right**, including the right to privacy, to be considered by the ECtHR in line with the **European Convention on Human Rights (ECHR) must cumulatively meet the following criteria:**

- interference shall be prescribed by law;
- interference shall pursue a legitimate aim;
- interference shall be necessary in a democratic society;
- interference shall be proportionate to the pursued purpose.

Thus, the information note on the draft law must cumulatively prove the way such criteria are grounded for any article or element of the Regulation affecting the right to privacy. The note on draft law no. 161 is deficient and provides no analysis of impact on human rights.

Any text that stipulates an interference must be clear and precise.

We emphasize the obligation that any interference with the right to privacy must be lawful, i.e. it must be "*prescribed by law"*, including the fact that the law must be of a certain quality. Thus, the ECtHR developed two main requirements: the law limiting the right to privacy must be sufficiently clear, precise and predictable, and beyond that it must be accessible.

Clarity, accuracy and predictability of law means that the law must be *"formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail"*[4].

In the particular context of interception of communications for the purpose of a police investigations, the ECtHR noted that, "*the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence"*[5].

Moreover, ECtHR considers that "*the substantive law itself, as opposed to accompanying administrative*

[4] ECtHR, Sunday Times *vs. The United Kingdom,* 26 April 1979, § 49.

[5] ECtHR, *Malone vs. The United Kingdom*, 2 August 1984, cited in the Council of Europe, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), p. 19.

practice, ***must indicate the scope and manner of exercise of any such discretion with sufficient clarity, having regard to the legitimate aim of the measure in question****, to give the individual adequate protection against arbitrary interference."*[6].

In this regard, we should note that in the proposed text unclear terms are often used, contrary to the international normative acts cited as motivation (for example, "provider of electronic mail services or text messaging", "suspending access", inclusion of traffic data and content data into the same category, obligation of keeping record of service users etc.), which does not meet the requirements for clarity in the normative acts texts. More comments in this respect are included in the specific observations below.

Texts of international documents should be corroborated by other related international normative acts

It seems that in the proposed text the provisions of international Conventions are taken literally and interpreted unilaterally, without taking into account their correlation with other related normative acts. For instance, the Budapest Convention on Cybercrime states in its Preamble the importance to correlate the Convention to other regulations and recommendations relating to the protection of privacy and personal data:

"- mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the ***1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms****, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy,*

- mindful also of the right to the protection of personal data, as conferred, for example, by the ***1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data****,*
(...)
- recalling Committee of Ministers Recommendations (...) ***No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (...)"***

Thus, all these provisions must be correlated to the way the Budapest Convention provisions are applied, an aspect which is entirely missing in the proposed text. Additionally, this International Convention cannot regulate details related to the way they are to be implemented, which are left with each member-state.

Thus, if the implementation of some articles of the Budapest Convention is desired, the provisions regulating the guarantees provided by the Convention should be implemented correlatively, or - if they already exist - references on how such provisions are already stipulated by the legislation of the Republic of Moldova.

In particular, the measures stipulated by the draft law no. 161 must be correlated with:

- respect for the right to privacy under the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1950) (see also p. I - The need for any interference with fundamental rights must be proved);
- legislation on protection of personal data, including rules on personal data protection in the police

[6] ECtHR, *Malone vs. The United Kingdom*, cited above.

sector.

Mass surveillance measures applied to all citizens violate the fundamental rights

In the current context of information society and following disclosures and reactions made public during the last 5 years, we need to make distinction between targeted surveillance (which may include interception of communications or access to meta-data) and mass surveillance that "does not begin with suspicion against certain person or persons"[7].

"Legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."[8] This is the conclusion of the European Court of Justice on mass surveillance - the opinion found in multiple decisions, studies and public statements that appeared, in particular, after disclosures by Snowden.[9]

Draft law no. 161 maintains, expands or introduces an obligation of general monitoring of all users of electronic communications "which is incompatible with fundamental rights, as concluded by several Constitutional Courts, for example the court of Germany[10], Romania[11], Czech Republic[12] or Slovakia[13], but also the CJEU in the decision as of 2014, ruling that:

"It must be stated that the interference with the fundamental rights (...) is wide-ranging, and it must be considered to be particularly serious. Furthermore, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned (...), the feeling that their private lives are the subject of constant surveillance".[14]

The European Union major normative acts that proposed or allowed mass surveillance measures had been already cancelled, such as the Directive on the retention of traffic data, as well as Safe Harbour Agreement for data transfer between the US and the EU.

Moreover, mass surveillance measures have never proved to be efficient. For example, the Parliamentary Assembly of the Council of Europe noted that according to "independent reviews carried out in the United States, mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials. Instead, resources that might prevent attacks are

---

7 For details see the Report of the Venice Commission as of March 2015, entitled "Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies" available at http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e.

8 CJEU decision in C-362/14 Maximillian Schrems/Data Protection Commissioner case http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117ro.pdf.

9 For a more comprehensive list see the chapter "Mass surveillance for the purpose of national security in international law" points 3- 16 of the Opinion of Decision PINTO DE ALBUQUERQUE in ECtHR, *Szabo and Vissy* v. Hungary, 12 January 2016 (http://hudoc.echr.coe.int/eng?i=001-160020).

10 Decision by the Constitutional Court of Germany (2010): http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.

11 See Decision 1258/2009 by the Constitutional Court of Romania- http://www.legi-internet.ro/jurisprudenta-it-romania/decizii-it/decizia-curtii-constitutionale-referitoare-la-legea-pentru-pastrarea-datelor-de-trafic-298-2008.html

12 Decision by the Constitutional Court of the Czech Republic (2011): http://www.usoud.cz/en/decisions/20110322-pl-us-2410-data-retention-in-telecommunications-services/.

13 Decision by the Constitutional Court of Slovakia (2014): http://fra.europa.eu/en/caselaw-reference/slovakia-constitutional-court-slovak-republic-pl-us-102014-78.

14 CJEU decision as of 8 April 2014 in Joined Cases C-293-12 and C-594-12 *Digital Rights Ireland.*

diverted to mass surveillance, leaving potentially dangerous persons free to act"[15].

Blocking of IP addresses by ISP is an Internet censorship

The requirement of blocking (in the original text the incorrect term "suspending" is used [16], for ex. art. VI of draft law no. 161 that amends art. 247[1] of the Contravention Code; art. VII l of draft law no. 161 that amends art. 7 letter h) of the Law on preventing and combating cybercrime) of some IP addresses by an Internet service provider (ISP) raises many issues of "privatized application of law" and creation of a censorship infrastructure, particularly in the context of ambiguity in regard upon who shall create and maintain this list and based on what criteria, but also issues of putting in the same category quite different situations from a technical standpoint (hosting vs. intermediary services).

The fundamental problem is that blocking websites via an Internet service provider is a measure of censorship of the online content, a measure that raises significant issues regarding observance of human rights in general and the right to freedom of expression in particular.

In this regard the European Union Directive for electronic communications stipulates the obligation for EU member states that access to the Internet cannot be blocked or limited abusively. Article 1 para. (3a) of the Directive 2002/21/CE expressly stipulates that:

> *"**Measures taken by Member States regarding end-users access' to,** or use of, services and applications through electronic communications networks **shall respect the fundamental rights and freedoms** of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law."*

Internet and websites are widely recognized as means of public communication, so blocking them arbitrarily is likely to contravene the ECHR and Art. 34 paragraph (5) of the Constitution of the Republic of Moldova, which states that "*The public media shall not be subject to censorship".*

The fact that draft law no. 161 stipulates unclear conditions when a specific site should not be accessed by users raises the issue of the constitutionality of this provision.

The lack of clarity in the text of the law regarding technical solutions for blocking (with different implications for privacy, as mentioned above) makes it impossible to study the proportionality of the measure of blocking the Internet. However, the ECtHR stated in its case law that even blocking of only certain sites is problematic and "does not diminish its significance, especially when the Internet has become one of the principal means by which individuals exercise their right to freedom of expression and information, the means providing essential tools for participation in activities and discussions of political issues of general interest."[17]

Also, the UN Rapporteur on freedom of expression concludes[18] on the subject that: **"*Blocking measures***

---

15 Para. 11 of Resolution No. 2045 (2015) of the Parliamentary Assembly of the Council of Europe, as of 21 April 2015, available at http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en.

16 Suspending access to an IP address - in the sense of stopping, cessation or interruption can be done technically only by the institution that manages IP addresses, in case of Romania it is RIPE NCC – https://www.ripe.net/, which has specific procedures for assignment or reassignment of IP addresses - https://www.ripe.net/publications/docs/ripe-643.

17 ECtHR, *Ahmet Yıldırım v. Turkey*, 6 April 2004 and *Cengiz and Others v. Turkey*, 1 December 2015.

18 Frank LaRue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", A.HRC.17.27,

***constitute an unnecessary or disproportionate means to achieve the purported aim*".**

From a technical standpoint, there are already worldwide documented cases in which, depending on the technical method used, blocking resulted in the impossibility of access to 100% legal websites, hosted on the same IP, or in blocking of the entire website (e.g. Wikipedia[19] or Tumblr[20]) for a single questionable content.

Moreover, implementation of such a system for blocking websites by Internet service providers means that a number of censorship tools that can be easily extended to other areas are created and operated. Once Internet blocking is accepted and once a technical system for its implementation is developed, more and more people will require more and more things to be censored.

In this context, in our view, the focus should be placed on identifying cases of child pornography on the Internet and deletion of this content (and not blocking it, which just means its concealment[21]), possibly by joining international networks of specific hotlines (see INHOPE). Also special efforts should be undertaken, in particular, to catch criminals who abused those children in real life, to prevent the recurrence of criminal acts.

Obligation to register some electronic services is at least questionable measure

Although the draft law no. 161 stipulates just adjacent issues to this subject, we consider important to note that the compulsory registration of users of some services under art. 7 of the Law on preventing and combating cybercrime no. 20-XVI of 03.02.2009 and establishment of penalties for failure to fulfil this obligation means that access to any electronic service is possible only after the user has registered in one way or another (the procedure which is not detailed).

Such an approach is, on the one hand, contrary to general principles of collecting personal data[22], imposing the obligation to register users, even if the provider of that service does not want it. On the other hand, such an obligation is illusory, as long as provision of services via Internet is not subject to any registration, so Moldovan citizens can at any moment apply to a provider outside the RM, circumventing these provisions. Moreover, there are services on the Internet where anonymity is a key aspect of the provision of those services - starting with VPN services or a service to report corruption or even reporting about child pornography content on the Internet.

The Internet is a decentralized space - the law could be unenforceable

Draft law no. 161 disregards the decentralized and not-state-limited structure of the Internet. Therefore, given that the Republic of Moldova is a relatively small actor in the Internet, too strict regulations will only lead to inapplicable legislation (foreign providers will refuse enforcement of some provisions that do not comply with

---

http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[19] See, for example, the case of the United Kingdom as of 2008, described here http://www.theregister.co.uk/2008/12/07/brit_isps_censor_wikipedia/.

[20] See, for example, the case of Italy as of 2013 - http://history.edri.org/edrigram/number11.4/italy-blocks-tumblr-domain.

[21] For more arguments see details at MOGIS - Remove, don't block! -- Act, and don't look away! - https://mogis.info/archive/eu/ro/**.**

[22] See in this regard the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, open for signature by the member States of the Council of Europe in Strasbourg on 28 January 1981, ratified by the Republic of Moldova and entered into force on 1 June 2008 (in particular Article 5), and Law no. 133 on the protection of personal data as of 8 July 2011 (in particular Article 4).

their national law) and sending of users from the Republic of Moldova to other services outside those national providers.

Furthermore, these measures (such as "keeping the records of service users" or "knowingly accessing adult pornography materials in public places") may operate to the detriment of companies providing online services and Moldovan citizens, as they are so easy to contravene.

Do you need a law amending so many aspects in one act?

From a formal standpoint, we emphasize that the way to adopt a normative act that amends other 7 normative acts[23] regarding the apparent implementation of several international conventions - some being mandatory, others being optional - from different domains (child protection, combating cybercrime etc.) raises questions about the effectiveness of this measure, especially with regard to the reasoning and debating of the draft law and the arguments on the need of their integration into a single normative act.

B. Specific opinions on the most important proposals to draft law no. 161

1. Art. II p. 4 (art. 259 para. (1) of the Criminal Code), p. 7 (art. 260^2), p. 8 (art. 260^3 para. (1)), p. 9 (art. 260^4 para. (1)), p. 11 (art. 260^6 para. (1)), p. 12 (art. 261^1 para. (1)) of draft law no. 161, providing for the exclusion of the following words from the enumerated paragraphs: words "(and) if these actions caused damages on a large scale."

We consider that limitation of cyber crimes only to those causing "large scale damages", as it is currently regulated, bodes well, given that the context of this offence is extremely broad and it is likely to receive many complaints that can flood the criminal prosecution bodies. For example, unauthorised "data interference" may cover a wide range of actions in practice, so prosecutors will have to discern in each case if the act presents a social threat that is large enough to be considered a criminal offence. Eventually, it needs to be discussed for which crimes such measure would be meaningful in terms of practice, after a detailed analysis of the typologies of crimes that would escape criminal proceedings. It is also possible to set a lower limit if it may be considered that there is a specific typology of offenses in Moldova.

In conclusion, we recommend maintaining the current text of the provisions of art. 259 para. (1), art. 260^2, art. 260^3 para. (1), art. 260^4 para. (1), art. 260^6 para. (1) and art. 261^1 para. (1), which include as element of a legally defined crime "if these actions caused damages on a large scale". Accordingly, art. II p. 4, 7, 8, 9 and 11 of draft law no. 161 have to be excluded or reconsidered.

2. Art. III p. 1, stipulating supplement of the Code of Criminal Procedure with article 130^1 worded as follows: "Article 130^1. Informatics search and seizure of objects that contain informatic data".

We suggest performing a detailed analysis of how this article shall be applied in order to provide a text that would strictly respect the right to privacy.

We also recommend supplementing art. 130^1 with the following:

[23] Draft law no. 161 amends the following normative acts: (1) the Criminal Code; (2) the Code of Criminal Procedure; (3) Law no. 264 as of 27.10.2005 on exercising medical professions; (4) Law no. 241 as of 15.11.2007 on electronic communications; (5) the Contravention Code; (6) Law no. 20 as of 03.02.2009 on preventing and combating cybercrime; (7) Law no. 59 as of 29.03.2012 on special investigation activity.

- In paragraph (5), regarding the expansion of a search for "another computer system or data storage device", we recommend application of the same procedural conditions as for the initial search, eventually including an element of celerity. **Given the fact that fundamental rights of a person are affected during an informatic search, it is important to preserve the level of authorization from the judge**, even if this may sometimes lead to the time extension of the criminal investigation. Given that in practice investigators do not search with an running computer system, mainly because it leads to inherent alterations of processed information, we estimate that such cases will be very few in practice, especially if it is desired to comply with the condition to be "accomplished through some technical means and methods that ensure the integrity and authenticity of the information contained therein."
- we recommend **inclusion of expressly stated obligation to make copies of all seized objects, at the moment of seizure and in the presence of witnesses and person who owns the data** and to analyse only them, to ensure the integrity of information data, and allow making real counter expertise at any stage of the proceedings and prove that the original data have not been altered in the process of seizure, storage or search (*chain of custody*). This obligation could be included in para. (3) of art. 130^1;
- given that the seized objects will in most cases contain and other information regarding private lives of individuals involved, as well as information that does not refer to the investigation for which the search is performed, **we consider that there should be an expressly stated obligation for the criminal prosecution bodies to keep confidentiality and return such data as soon as it is found that they are not relevant to the case under consideration**, so that these information does not become public unreasonably. Obligation to keep confidentiality and return such data immediately shall be expressly provided by art. 130^1 of the Code of Criminal Procedure.

3. Art. III, p. 2, which provides for the extension of a series of special investigation measures applied to all grave, especially grave or exceptionally grave crimes and a number of less serious offences. Namely, it is proposed to apply the following special measures of investigation stipulated by the Code of Criminal Procedure (CCP):

- domicile searches and/or installation audio, video, photo, filming equipment therein (art. 132^6 CCP),
- domicile surveillance using technical means (art. 132^7 CCP),
- documentation by means of technical methods and devices, localization or surveillance by means of global positioning system (GPS) or by other technical means (art. 134^3 CCP, *note: carried out only with the authorization of the prosecutor under art. 132^2 CCP*),
- withholding, investigation, transfer, search or seizure of postal items (art. 133 CCP),
- identification of the subscriber, owner or user of the electronic communication system or access point to an information system (art. 134^5 CCP, *note: carried out only with the authorization of the prosecutor under art. 132^2 CCP*),
- gathering of information from electronic communication services providers (art. 134^4 CCP),
- visual tracking (art. 134^6 CCP, *note: carried out only with the authorization of the prosecutor under art. 132^2 CCP*),
- test purchasing (art. 138^3 CCP, *note: carried out only with the authorization of the prosecutor under art. 132^2 CCP*),
- covert investigation (art. 136 CPP, *note: carried out only with the authorization of the prosecutor under art. 132^2 CCP*),
- transboundary surveillance (art. 138^1 CCP, *note: carried out only with the authorization of the prosecutor under art. 132^2 CCP*),

To the following crimes:

- there is a reasoned suspicion for preparation or commission of a grave, especially grave or exceptionally grave offence, under exceptions provided by the law OR in case of offences stipulated by

- art. 174 - Sexual intercourse with a person under the age of 16,
- art. 175 – Perverted actions,
- art. 175^1 – Seduction of a minor for sexual purposes,
- art. 185^1 – Violation of copyright and related rights,
- art. 185^2 – Violation of industrial property rights,
- art. 208^1 – Child pornography,
- art. 208^2 - Resorting to prostitution practiced by a child,
- art. 237 – Production or putting into circulation of false cards or other pay checks,
- art. 259 - Illegal access to computerized information,
- art. 260 - Illegal production, importing, marketing, or putting at disposal of technical means or software products,
- 260^1 - Illegal interception of an information data transfer.

While detailing the norms provided under art. III p. 2 of draft law no. 161, it is obvious the legislator wanted to expand the list of offences for which special investigation measures can be applied, including those applied only when authorized by the prosecutor.

In our view, the **extension** of these measures to an extremely large category of serious and less serious crimes **shall be justified in particular, for each separate crime**, because we are dealing with an extension of the limitation of fundamental rights that cannot be justified generically in accordance with the consistent practice of the ECtHR.

At the same time it is obvious that **certain crimes from this list** (such as those of "illegal access to computerized information", "mere possession of child pornography" or those related to the violation of the copyright can easily be used for other purposes or relatively easily carried out by anyone and, especially in this context, **do not seem to have the severity** stipulated for such measures by law, therefore, can be used unjustifiably very easily.

In conclusion, we recommend to limit the list of crimes for which special investigation measures can be applied, i.e. modification of art. III p. 2 of draft law no. 161.

4. Art. III p. 3, stipulating supplement of Article 138^2 of the Code of Criminal Procedure (controlled delivery) with paragraph (7) worded as follows: "A special investigation measure stipulated under this article can be ordered in case of offences under art. 132^1 para. (2) p. 2) of this Code or in case of an offence under art. 175^1, 185^1 -185^2, 208^1, 208^2, 237, 260-260^2, 260^4, 260^6 şi 261^1 of the Criminal Code."

We consider that the list of crimes for which it is allowed to apply the special investigation measure "controlled delivery" is too broad and should be reviewed and limited accordingly. Thus, under art. III p. 3 of draft law no. 161 it is proposed to order special investigation measure controlled delivery in any case when there is a reasoned suspicion regarding the preparation or commission of a grave, especially grave or exceptionally grave crime under exceptions stipulated by the law or in case of the following offences stipulated by the Criminal Code:

- 175^1 – Seduction of a minor for sexual purposes;
- 185^1 – Violation of copyright and related rights;
- 185^2 – Violation of industrial property rights;
- 208^1 – Child pornography;
- 208^2 - Resorting to prostitution practiced by a child;

- 237 – Production or putting into circulation of false cards or other pay checks;
- 260 - Illegal production, importing, marketing, or putting at disposal of technical means or software products;
- 260^1 - Illegal interception of an information data transfer;
- 260^2 - Alteration of integrity of the data held in an information system;
- 260^4 - Illegal production, importing, marketing, or putting at disposal of passwords, access codes or similar data;
- 260^6 - Computer fraud and
- 261^1 - Unauthorized access to telecommunications networks and services.

The author of the draft law failed to explain the need to provide for such an intrusive investigation measure for all these crimes. In particular, the inclusion of this measure for offences related to copyright is not clear (art. 185^1 and 185^2). We recommend reviewing the entire list, providing justification for crimes maintained, and exclusion of art. 185^1 and 185^2 from the list of crimes for which controlled delivery can be used.

5. Art. III, p. 6 of the draft no. 161, which provides for the introduction of a new type of special investigation measure – interception and recording of information data - amending art. 132^{11} of the CCP (that currently stipulates verification of the interception recording) by including the following norms:

"Article 132^{11}. Interception and recording of information data

(1) Interception and recording of information data that consists in the use of some technical methods and/or means intended to collect real time data on information traffic and/or data on the content related to communications in question, other than those provided under art. 132^8, transmitted through a computer system, and storage of information obtained during interception on technical support device.

(2) Interception and recording of information data shall be ordered and carried out under the conditions set out in art. 132^9 that are applied accordingly[24].

(3) A special investigation measure established under this article can be ordered in case of crimes under art. 132^1 para. (2) p. 2) of this Code or in case of an crime under art. 175-171^1, 185^1-185^3, 208^1, 208^2, 237 and 259-261^1 of the Criminal Code."

Article 132^{11} stipulated under art. III. 6 of the draft law no. 161 is unclear in terms of the necessary distinction between traffic data and content data, especially regarding the distinction between content data under art. 132^{11} and communication data under art. 132^8 of the Code of Criminal Procedure. **It is in this perspective logical that some clear and unequivocal distinction should be made between:**

- **content of communications**, for which interception is already regulated under art. 132^8; Technically speaking, a communication via IP protocol is "content data", and
- **traffic data**, that appear to be already regulated under art. 134^4.

Even the Budapest Cybercrime Convention makes clear distinction between these two types of data (Art.20 and Art.21 respectively).

In this context we must emphasize that **the provisions of the Budapest Cybercrime Convention should not be implemented literally,** but there should be institutions acting under national law, which authorise such procedural measures, taking into account national experiences. At the same time these measures should be circumscribed to the ECtHR practice and national constitutional provisions, so in our opinion, measures related to traffic data (art. 134^4 of the Code of Criminal Procedure and art. 7 of the Law on preventing and combating

[24] Art. 132^9 CCP provides for the execution and certification of interception and recording of communications by the criminal prosecution body or investigation officer, with the authorization of the court investigator.

cybercrime) should be reviewed in the context of constitutional decisions[25] and those of the European Court of Justice for the past 2 years[26].

Thus, **we recommend waiving any generalized measure with regard to the obligations of retaining traffic data**, which were consistently declared to be contrary to the fundamental rights. We recommend reviewing of art. 132[11] restricting its applicability only to the interception of content data, applied under conditions and limits similar to those related to the interception of electronic communications.

6. Art. III p. 8 of draft law no. 161 that stipulates introduction to Art. 133 of the Criminal Code, to the title, after the words "postal items" the words "and electronic communications"; *in paragraph (1), after the words "postal items" shall be introduced the text "and / or electronic communications"; in paragraph (2), after the words "postal items" shall be introduced the text "and / or electronic communications", but after the word "fax" shall be introduced the text "textual messaging by means of information systems besides telephone services"; in paragraph (3), after the words "postal items" shall be introduced the text "and / or electronic communications", after the words "postal institution" shall be introduced the text "or, where appropriate, the provider of email or textual messaging service", and after the words "postal items" shall be introduced the text "and / or electronic communications"; in paragraph (4), after the words "postal institution" shall be introduced the text "or, where appropriate, the provider of email or textual messaging service"; in paragraph (5), after the words "postal institution" shall be introduced the text "or, where appropriate, the provider of email or textual messaging service"; in paragraph (6), after the words "postal items" shall be introduced the text "and / or electronic communications".*

In our opinion withholding, investigation, transfer, search or seizure of postal items should be regulated differently from any form of electronic communication, given their different technical nature and distinct nature of the typology of services:

- postal services are strictly regulated and provider controls the entire process;
- electronic communication services are regulated, but in some cases the provider has no control over the services to which it allows access, depending on the fact if it is a provider of telephone communications, cable television or Internet service providers;
- online services (or information society services) - such as, resulting from the above text, services of "*textual messaging by means of information systems besides telephone services*" or "*electronic mail*" - which are relatively less regulated, can be centralized or decentralized, encrypted or not, with the encryption key on the server or with an end-to-end encryption from[27].

In this context we should also point out that the use of some terms related to the specificity of a means of communication (as fax, electronic mail or text messaging) disregards the principle of technological neutrality and are likely to end up like "telegraph" in the modern context. Therefore, we consider that electronic communications are to be regulated under articles separate from those of the postal communications, and with

[25] We refer to decisions of the courts from Germany, Romania, Czech Republic and Slovakia on the issue of traffic data - already cited in footnotes. 8. A comprehensive list on the situation in several Member States can be found here - http://wiki.vorratsdatenspeicherung.de/Transposition.

[26] For example, CJEU decision in the case C-362/14 Maximillian Schrems/Data Protection Commissioner http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117ro.pdf; CJEU decision as of 8 April 2014 in Joined Cases C-293-12 and C-594-12 *Digital Rights Ireland http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=RO*.

[27] For details see Bogdan Manolea, The end-to-end principle of the Internet and its implications upon the law - http://legi-internet.ro/blogs/index.php/principiul_end_to_end_al_internetului_si.

regard to electronic communications generic notions and framework concepts should be used, such as:

- interception of electronic communications, whether voice or text, whether email, chat, text messaging or video messaging; and
- access to traffic data, that do not include the contents of communications and that can be less intrusive.

Additionally, the type of obligations should be directly linked to the category of provided services. At the same time, we warn on the possibility of over-regulation, but also of inapplicable regulation (see points VI and VII, section A above), which would ultimately lead to unresolved substantive issues related to cybercrime.

Accordingly, we recommend excluding of art. III p. 8 from the draft law no. 161, which provides for the inclusion of the phrase *"and electronic communications"* to art. 133 of the Code of Criminal Procedure, making a dangerous confusion between electronic communications and postal communications and ways of access to them.

7. Art. VI p. 1 of the draft law no. 161, which stipulates that the provision of article 90 of the Contravention Code[28] shall be supplemented at the end by the text "or knowingly accessing them in public places".

In most European states, adult pornography materials fall into the lawful content category, but potentially harmful for minors (*harmful content*). In this context, the emphasis should be placed on non-legislative measures that would not allow children to access this content, as well as on effective education measures rather than on legislative restrictions for this type of content, which anyway are illusory in case of the Internet. Children can accidentally access pornographic content in any place with access to the Internet - whether public or not. Therefore, the solution must be correlated directly with the problem.

The following materials are relevant to this end:

- Council of Europe - Protecting children against harmful content (2013) - https://edoc.coe.int/en/children-and-the-internet/5779-protecting-children-against-harmful-content.html
- Reports and recommendations by the EU's main research project on this topic – EU Kids online http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Accordingly, we recommend waiving the introduction of penalties for knowingly accessing adult pornography materials by adults in public places and, therefore, exclusion of Art. VI p. 1 from the draft law no. 161

8. Art. VI p. 2 of the draft law no. 161, which provides for supplementing the Contravention Code with article 247[1] worded as follows: Article 247[1]. Violation of legislation on preventing and combating cybercrime. Violation of legislation on preventing and combating cybercrime by providers of electronic communication services, regardless of the type of property and legal form of organization, evidenced by ... ".

We will refer below to several actions included in art. 247[1] of the Contravention Code which are problematic and should be either excluded or reformulated.

I.1. "a) failure to fulfil the obligation on keeping records on service users;"

[28] Current provision of art. 90 of the Contravention Code stipulates: „Producing, selling, distributing and keeping pornographic products for sale or distribution."

Obligation under letter a) of art. 247^1 of the Contravention Code is extremely vague and unclear, given that it is not sufficiently clear about what type of services we speak. It also seems that the obligation is based on the premise that there is no right to communicate anonymously (for details see p. VI of section A of the opinion).

Accordingly, we recommend to waive this provision or clarify it for certain categories of service providers, so that they also can adapt their behaviour to comply with the law.

I.2. "b) failure to inform competent authorities about illegal access to information from the information system, about attempts to introduce illegal programmes, violation by responsible persons of rules for collecting, processing, storage, dissemination, distribution of information or protection rules of the information system provided in accordance with the status of information or its degree of protection, if they contributed to the acquisition, distortion or destruction of information or caused other serious consequences, disrupting the operation of information systems, other incidents related to information security with significant impact;"

There is a worldwide reluctance in reporting cyber crimes to competent prosecution authorities. The main motivation lies in the contradiction between the fact that the criminal proceedings will get into a public phase and the need for protection of data or image of a company or a person. In this regard, the authorities should focus more on fostering collaboration and not on penalizing non-collaboration.

At the same time the level where such reporting becomes mandatory should be made explicit, not to leave this decision for the affected (we refer in particular to the terms "*other serious consequences; "disrupting the operation of information systems"* or *"other incidents related to information security with significant impact"*.)

Thus, we recommend to reconsider the penalty for non-collaboration, providing for voluntary collaboration or limiting sanctions for non-reporting to a narrower circle of subjects and clarify terms used in art. 247^1 letter. b) of the Contravention Code (unclear terms: "other serious consequences; "disrupting the operation of information systems", "other incidents related to information security with significant impact"*).*

I.3. "f) failure to retain traffic data, as stipulated under the law, with the view to identify service providers, service users and the channel through which communication was sent;"

This obligation, as formulated in the draft law no. 161, is actually a generalized obligation to retain traffic data, thus being a mass surveillance measure and creating preconditions for violation of the right to privacy. (see the context explained in p. IV section A of the opinion above).

In the context of the CJEU decisions Digital Rights Ireland and Schrems, as well as decisions of the Constitutional Court referred to in chapter IV above and point 5 above, we recommend waiving this provision of mass surveillance.

I.4. "g) failure to fulfil the obligation on suspending, using available technical methods and means, as stipulated under the law, access to all IP addresses, including those hosted by the provider concerned, on which webpages are located containing child pornography, promoting sexual abuse or sexual exploitation of children, containing propaganda information for war or terrorism, urging to hatred or ethnic, racial or religious discrimination, to hostility or violence, containing or disseminating instructions on how to commit crimes,"

This obligation may violate the right to freedom of expression, but also the right to privacy, depending on

technical implementation - see the context explained in p. V section A of the opinion.

Nevertheless, the phrase „suspending access to all IP addresses on which webpages are located“, is incorrect also from technical point of view – starting with the fact that the correct term is blocking, as well as the fact that a website or multiple websites can be hosted on the same IP address, up to the fact that in the context of current information technology development when data are hosted by intermediaries – a type of cloud computing service or Content Distribution Network (CDN)[29] - access to an indicated IP address might not at all block wanted content and instead will block unwanted content.

Moreover, the phrase "information urging to hatred or ethnic, racial or religious discrimination“ is too general - based on it access to Facebook, YouTube and Twitter should be blocked, as they certainly contain such information.

Also the phrase “containing or disseminating instructions on how to commit crimes” is extremely vague and dangerous. To give just one trivial example: only on YouTube there are 76 000 videos[30] that show how to open a door without a key.

Also it is not clear who determines that an IP address should be blocked, what possibilities of appeal do exist, as well as other practical details that make such measure create more premises for censorship than have any positive effect.

In the context of these vague terms, but also considering the ECtHR decisions in case of *Ahmet Yıldırım v. Turkey* and *Cengiz and Others v. Turkey*, and other arguments set out in chapter V above, we recommend exclusion from the draft law no. 161 of the obligation of „suspending access to all IP addresses on which webpages are located“, proposed in letter g) of the Contravention Code.

9. Art. VII of the draft law no. 161 provides a number of amendments to Law no. 20 as of 3 February 2009 on preventing and combating cybercrime. Below we shall refer to the most problematic ones, providing necessary recommendations.

In the context of the law on cybercrime for solving the current the problems related to cyber crimes, we think one needs to focus on activities of overall understanding of the phenomenon, including sociological or criminological points of view. In this respect inter-state international cooperation activities are recommended, and also those contributing to the development of the necessary human resources to focus on the issue of cybercrime, rather than introducing vague and problematic provisions.

9.1. Art. VII, p. 4. of draft law no. 161 provides that "Article 5 shall be supplemented by paragraph (2) worded as follows: "(2) Service providers, non-governmental organisation, civil society representatives and any other persons are encouraged to submit to the Inspectorate General of Police and Prosecutor General's Office any information which become known to them regarding natural and /or legal persons that distribute, broadcast, import or export images or other representations of one or more children involved in sexual activities, as well as regarding sexual abuse against a child using electronic communications. "

[29] See the explanation of the concept and a list of major providers at https://en.wikipedia.org/wiki/Content_delivery_network

[30] See an example here: https://www.youtube.com/results?search_query=how+to+open+a+locked+door+without+a+key

Although this is a direction supported worldwide, especially for reporting on child pornography materials distributed through computer networks, it is very likely not to be effective when even mere possession is considered a criminal offence.

In this regard we recommend decriminalization of „mere possession“ to allow reporting of illegal content to the relevant authorities. This is the purpose of limitation in art. 9 (4) of the Budapest Convention which allows member-states to incriminate "mere possession". Moreover, not all signatories to the Budapest Convention have incriminated such a crime.

9.2. Art. VII p. 5 of draft law no. 161 stipulates amendments to art. 6^1 of Law no. 20 and namely: “d) to inform competent authorities immediately, but not later than 24 hours since the moment of detection about illegal access to information from one's own information system, about attempts to introduce illegal programmes, violation by responsible persons of rules for collecting, processing, storage, dissemination, distribution of information or protection rules of the information system provided in accordance with the status of information or its degree of protection, if they contributed to the acquisition, distortion or destruction of information or caused other serious consequences, disrupting the operation of information systems, other incidents related to information security with significant impact.”

As we mentioned above, while analysing the proposal of the draft law regarding art. 247^1 letter b) of the Contravention Code, there is a worldwide reluctance in reporting on cybercrime to competent prosecution authorities where the main motivation lies in the contradiction between the fact that the criminal proceedings will get into a public phase and the need for protection of data or image of a company or a person. In this regard, the authorities should focus more on fostering collaboration and not on penalizing non-collaboration.[31]

Eventually, it may be required reporting only for limited categories of crimes where social danger and identification of cases to be reported is clear for all subjects of law- e.g. Crimes against information systems of critical infrastructures belonging to the State (if they are defined in other normative acts) or Crimes against information systems belonging to banks.

At the same time the level where such reporting becomes mandatory should be made explicit, not to leave this decision up to the subjectivity of the affected (we refer in particular to the terms “*other serious consequences; “disrupting the operation of information systems” or “other incidents related to information security with significant impact”*.) The subject is closely related to other similar notifications, but with smaller consequences for private operators (see notifications on security breaches in the domain of personal data protection) where many good and bad practices on this topic are identified.[32]

In conclusion, we recommend reconsidering and rewriting this article, given the objective to encourage the reporting of crimes voluntarily.

It should be also explained what competent authorities mean and what is the purpose of reporting, it can be viewed from 3 different points:

- reporting to criminal prosecution bodies to identify and punish the criminals,

[31] See also the Best practices of the Department of Justice of the USA as an example in this regard - https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf

[32] For example, see the report by ENISA - Data breach notifications in the EU https://www.enisa.europa.eu/publications/dbn

- reporting to information security bodies (e.g. a unit of CERT type) for stopping or reducing the effects of information security breach (see the 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 (NIS Directive)[33])
- reporting to the authorities in the domain of personal data protection for the purpose of informing of affected persons (see EU regulation on the protection of personal data[34] – to be implemented in all EU Member States since 2018).

9.3. Art. VII, p. 6 of the draft law no. 161 stipulates amendments to art.7 of Law no. 20, and namely: (1) letter a) shall be amended at the end with the text "but in the case of anonymous prepaid services - date and time of the initial activation of the service"; letter b) the text "data on information traffic, including" shall be replaced by the text „under Art. 4 para. (1)" and the words "information offences" shall be replaced by the words "incidents related to information security with significant impact";

These data (Date and time of the initial activation of anonymous service, data on information traffic and incidents related to information security with significant impact) constitute traffic data collected in a generalized and unjustified way (see comments above on those aspects of traffic data retention chapter IV section A of the opinion).

In the context of the CJEU decisions Digital Rights Ireland and Schrems, as well as decisions of the Constitutional Court referred to in chapter IV, we recommend waiving this provision of mass surveillance.

9.4. Art. VII, p. 6 of the draft law no. 161 stipulates amendments to art. 7 of Law no. 20, and namely: (1) letter c), the word "immediately" is replaced with the word '„quickly", after the words "information traffic" the following text is inserted "indicated in that request" and the text "120 calendar days" is replaced by "180 calendar days";

Any extension of legislation affecting fundamental rights must be accompanied by an analysis of the need for interference in a democratic society. In this case the extension of the term by two months is not justified in any way.

Moreover, we should recall that the European directive 2006/24/EC providing for a period of 6 months was considered excessive and violating the fundamental rights of the EU citizens. Therefore, in the context of the CJEU decisions Digital Rights Ireland and Schrems, as well as decisions of the Constitutional Court referred to in chapter IV, this issue should be reviewed completely.

Accordingly, we recommend complete waiving of any measure of retaining traffic data that is including this amendment.

9.5. Art. VII, p. 6 of the draft law no. 161 stipulates amendments to art. 7 of Law no. 20, and namely: paragraph (1) letter f), the text "monitoring, surveillance and" shall be excluded, and the text "for a period of 180 calendar days" shall be replaced by "for the network of fixed telephony and mobile telephony for a period of one year and those related to Internet traffic and Internet telephony - for a period of six months";

Any extension of legislation affecting fundamental rights must be accompanied by an analysis of the need for

[33] See the NHIS Directive here: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148.

[34] Full text available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

interference in a democratic society. In this case the extension of the term is not justified in any way.

Moreover, we should recall that the European directive 2006/24/EC providing for a period of 6 months was considered excessive and violating the fundamental rights of the EU citizens. Therefore, in the context of the CJEU decisions Digital Rights Ireland and Schrems, as well as decisions of the Constitutional Court referred to in chapter IV, this issue should be reviewed completely.

Accordingly, we recommend complete waiving of any measure of retaining traffic data, that is including this amendment.

9.6. Art. VII, p. 6 of the draft law no. 161 stipulates amendments to art. 7 of Law no. 20, and namely: paragraph (1) „h) to suspend, using available technical methods and means, as stipulated under the law, access from one's own information system to all IP addresses, including those hosted by the provider concerned, on which webpages are located containing child pornography, promoting sexual abuse or sexual exploitation of children, containing propaganda information for war or terrorism, urging to hatred or ethnic, racial or religious discrimination, to hostility or violence, containing or disseminating instructions on how to commit crimes".

Obligation to „suspend access" proposed under art. 7 para. (1) letter h) may violate the right to freedom of expression, but also the right to privacy, depending on technical implementation. See also detailed context in p. V (blocking of IP addresses) and comments in p. VIII.4 above.

According to the feedback presented to this opinion by the Information Centre for Combating Cybercrimes, the following wording to art. 7 paragraph. (1) h) was proposed within discussions of the draft law no. 161 in the Parliamentary Committees,

"h) suspend under the law, using technical means and methods in possession, the access from one's own information system to the webpages that are located web pages, including those hosted by the provider concerned, containing child pornography, promoting sexual abuse or sexual exploitation of children, containing propaganda of war or terrorism, calls for hatred or discrimination on ethnic, racial or religious hostility or violence."

Art. 7 was supplemented with par. 3 with the following wording: *" (3) The interruption of access to websites, in para. (1) h) of this Article, shall be ordered by the court in criminal cases, where the service provider has removed from the websites hosted on or under his control such information at the request of the law enforcing bodies or if the determination of the contact details of the service provider was not possible. 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, is ordered by the law enforcement bodies in accordance with the List drawn up by the International Criminal Police Organisation (Interpol 'Worst of' -List), made available to the service provider."*

Unfortunately even the text proposed by the Parliament does not clarify thess issues, mentioning confusingly in the same article the term of service provider who has hosted web pages and interrupting access to web pages. A service provider could be both an Internet access provider and a hosting provider, but each has different responsibilities. Moreover, details from this version - the reference to the list of "Worst-of" Interpol - shows that not all technical options have been sufficiently analysed. Thus, thie mentioned list blocks domains, and not web pages or IP addresses, that raises another range of problems.

Also this new article sets regulates diametrically opposite solutions - in the first subparagraph blocking is ordered by the court, but in the second by the “law enforcement bodies” according to an international list that exceeds national legal framework (which is more a “soft law”).

In the context of the extremely vague text and ECtHR decisions in case of Ahmet Yıldırım v. Turkey and Cengiz and Others v. Turkey, no. 48226/10 and 14027/11, 1 December 2015, and other arguments set out in p. V of the opinion, **we recommend exclusion from Law no. 20 of the provision that allows and requires „suspending of access”.**

9.7. Art. VII p. 7 of the draft law no.161 stipulates amendments to art. 10 of Law no. 20 and namely proposes to amend para. (5) as follows: "(5) If, while fulfilling of a request for retaining data on traffic, the competent authority of the Republic of Moldova discovers that a service provider has participated in transmission of this communication in another state, it will rapidly reveal to requesting foreign competent authority sufficient amount of data on traffic with the view to identify that service provider and the channel through which the communication was transmitted."

The text could be interpreted as meaning that a service provider from the Republic of Moldova may reveal to a foreign public authority information which can be of a personal nature (traffic data) without any procedural guarantee in this case. We consider that the wording should be clarified in the context of an explanation of the need for addition of this article.

We would recommend, first of all, to specify expressly the need to introduce this specific article in the note to draft law no. 161 and revise the text of the article to specify that information that can be transmitted abroad shall not contain personal data, which could eventually be disclosed only under the authorization of a judge, as provided by the legislation of the Republic of Moldova.