The International Center for Not-for-Profit Law
1126 16th Street NW, Suite 400
Washington, DC 20036
Contact: Zach Lampell, Legal Advisor
zlampell@icnl.org

In March 2016, the Republic of Moldova's Ministry of Internal Affairs promoted the Draft Law for Amending and Completing Some Legislative Acts, which addresses online behavior by criminalizing certain actions and providing government authorities with additional surveillance and investigatory powers. This Draft Law (Amendments) were approved by the Government of the Republic of Moldova and submitted to the Moldovan Parliament for review and examination.

The Amendments seek to amend eight laws[1]: (1) the Law on the Intelligence Service of the Republic of Moldova; (2) the Criminal Code of the Republic of Moldova; (3) the Criminal Procedure Code of the Republic of Moldova; (4) the Law on Performing the Profession of Medical Doctor; (5) the Law on Electronic Communications; (6) the Code for Contraventions; (7) the Law on Preventing and Fighting Against Computer Crimes; and (8) the Law on Special Investigation Activity.

At the request of local partners, ICNL has developed an overview of the possible implications to the freedom of expression and right to privacy, should the proposed Amendments be adopted in the current form. The issues are reviewed against the backdrop of international standards and existing good practices. ICNL stays available to follow further developments with the Amendments and provide technical assistance to the stakeholders to ensure that illegal acts online are prevented without restrictions to the fundamental freedoms and rights.

ICNL is concerned that the Amendments contain provisions that may potentially have a chilling effect on the freedom of expression and right to privacy. As drafted, the Amendments violate international standards guaranteeing these fundamental rights. Key concerns include the following:

- **Vague Grounds to Block Websites**. The Amendments permit authorities to block access to websites for vague reasons, including if such websites contain "information propagating war or terrorism, calls to hate or national, racist or religious discrimination, to hostility and violence, containing or distributing instructions on how to commit crimes."[2] Vague language such as this may invite arbitrary and subjective application,

[1] There is some concern with the way these multiple amendments to the laws were introduced, as they address various issues and might be used for subjective interpretation on certain occasions.
[2] Amendments, Article VI(2)(g) – Amendment to the Code for Contravention, Article 247[1] and Article VII(6) – Amendment to the Law on Preventing and Fighting Against Computer Crimes, Article 7(1)(h).

resulting in violations of the freedom of expression.

- **Lack of Judicial Oversight.** The Amendments provide broad powers for law enforcement to search and seize equipment and data without meaningful judicial oversight. The lack of judicial oversight is likely to lead or contribute to an impermissible restriction on the freedom of expression and right to privacy.[3]

- **No Protection for Whistleblowers or Journalists.** The Amendments criminalize legitimate actions, including certain acts and tools that journalists, whistleblowers and other public watchdogs need to use in their role as monitors of governmental activity.

The Freedom of Expression and Right to Privacy in International Law

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) requires State parties to guarantee the right to freedom of expression, including the right to receive and impart information and ideas of all kinds regardless of frontiers. The full text of Article 19 reads:

> 1. Everyone shall have the right to hold opinions without interference.
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

Article 19 of the ICCPR requires State parties to guarantee the right to freedom of expression, including the right to privacy and the right to receive and impart information and ideas of all kinds regardless of frontiers.[4] The Human Rights Committee has stated that, "any restrictions on the operation of websites, blogs, or any other internet-based electron or other such information dissemination systems" must comply with Article 19.[5] Restrictions to the speech and expressions guaranteed in Article 19 are lawful only when such restrictions pass a three-part, cumulative test:

[3] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 56, UN Doc. # A/HRC/23/40, (April 2013).
[4] The Republic of Moldova acceded to the ICCPR on January 26, 1993.
[5] Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression, para. 43, UN Doc # CCPR/C/GC/34 (2011).

> (1) the restriction must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);
> (2) the restriction must pursue one of the purposes set out in article 19(3) of the ICCPR, namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and
> (3) the restriction must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).[6]

Similarly, the right to privacy is enshrined in Article 17 of the ICCPR, "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." The right to privacy rests on the underlying premise that individuals have a "private sphere" where they can interact free from State intervention.[7] "In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous."[8]

Although Article 17 envisages necessary, legitimate and proportionate restrictions to the right to privacy, the Special Rapporteur for Freedom of Expression (Special Rapporteur) states that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, elucidated in the Human Rights Committee General Comment 27, paragraph 15:

> (a) Any restrictions must be provided by the law;
> (b) The essence of a human right is not subject to restrictions;
> (c) Restrictions must be necessary in a democratic society;
> (d) Any discretion exercised when implementing the restrictions must not be unfettered;
> (e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims. It must be necessary for reaching the legitimate aim; and
> (f) Restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected.[9]

---

[6] S*ee, e.g.*, Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 69, UN Doc. # A/HRC/17/27 (May 2011).
[7] *See*, Lord Lester and D. Pannick (eds.). Human Rights Law and Practice. London, para. 4. 82 (Butterworth, 2004).
[8] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 23, UN Doc. # A/HRC/23/40 (April 2013).
[9] Human Rights Committee, General Comment No. 27: Freedom of Movement (Article 12), para. 15, UN Doc # CCPR/C/21/Rev.1/Add.9 (1999); Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 29, UN Doc. # A/HRC/23/40 (April 2013).

The freedom of expression and the right to privacy are interrelated, "the right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression."[10] Limitations or restrictions to one of these rights impact the enjoyment of the other. Just as a restriction to the freedom of expression must pass the three-part cumulative test derived from ICCPR Article 19 to be lawful, a restriction to the right to privacy is only lawful if it passes the test articulated in General Comment 27.15.[11]

ANALYSIS

Blocking of Websites

Issue: Article VI(2)(g) obligates all "suppliers of electronic communication services" to block all websites "containing child pornography, promoting sexual abuse or sexual exploitation of children,[12] containing information propagating war or terrorism, calls to hate or national, racist or religious discrimination, to hostility and violence, containing or distributing instructions on how to commit crimes." If these suppliers of electronic communication services do not block these websites, they are liable to be fined.

A similar provision is found in Article VII(6), which amends the Law on Preventing and Fighting Against Computer Crimes. The relevant provision of that article states that "[internet] service providers shall: suspend…the access from its own computer system to all the IP addresses on which webpages are located, including the ones hosted by the respective supplier, containing … information propagating war or terrorism, calling to hate or national, racial or religious discrimination, to hostility or violence, containing or disseminating instructions about how to commit crimes."

Analysis: This provision likely fails parts 1 and 3 of Article 19's three-part test. The first part of the three-part test requires restrictions to the freedom of expression to be both predicable and transparent. While this provision meets the transparency requirement because it is accessible by everyone, it is not predicable for two reasons. First, the term "suppliers of electronic communication services" is undefined, thus making it unclear which individuals or entities are subject to this provision; and second, the use of vague language such as "calls to hate" and "containing or distributing instructions on how to commit crimes," are vague and unclear.[13]

---

[10] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 24, UN Doc. # A/HRC/23/40 (April 2013).

[11] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 29, UN Doc. # A/HRC/23/40 (April 2013).

[12] The Government of Moldova should be commended for protecting children from sexual exploitation, and indeed child pornography is one clear area where blocking measures can be justified. However, the law allowing for internet blocking must be "sufficiently precise" and there must be "effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body." See, Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 32, UN Doc. # A/HRC/17/27, (May 2011).

[13] See e.g., *Ahmet Yildirim v. Turkey*, European Court of Human Rights, Judgment, 18 December 2012, concluding that blocking measures based on vague terms fail to meet the foreseeability requirement in Article 10 of the

Article VI(2)(g) also likely fails the third prong of Article 19's three-part test because blocking entire websites is not least restrictive way to achieve the purported aim of protecting national security or public order. If adopted as drafted, the aforementioned provisions give authorities broad latitude to force private entities to block access to many different websites, which constitutes an extreme threat to the freedom of expression.

Furthermore, this article seeks to impose intermediary liability, which violates the right to freedom of expression. This constitutes a form of censorship, and "censorship measures should never be delegated to a private entity, and that no one should be held liable for content on the Internet of which they are not the author."[14] Article VI(2)(g) runs afoul of both these principles.

Finally, neither this article nor any other article in the Amendments contain specific instructions on how authorities will determine when these websites are to be blocked, or if an independent judicial authority must approve such blocking. Without adequate judicial oversight, there is greater concern for abuse.

Recommendation: Article VI(2)(g) should be re-drafted so that the grounds for blocking access to websites are clear and specific, with precise, objective criteria for determining how and when the blocking of websites is to take place, with adequate and meaningful judicial oversight.

Lack of Judicial Oversight

Issue: The Amendments give law enforcement the ability to search and seize equipment and data without meaningful, judicial or other independent oversight.

Specifically, proposed Article 130[1] of the Code of Criminal Procedure[15] permits the search and seizure of computer data, but allows for such search and seizure only via a "reasoned order of the prosecutor" in a number of instances. Similarly, proposed Article 4 of the Law on Preventing and Fighting Against Computer Crimes grants the General Prosecutor's Office, General Police Inspectorate and the Intelligence Service broad powers to collect, store, search and seize computer data.[16] Very few, if any, instances of such collection, conservation or searching require approval from a judicial body.

The Law on the Intelligence Service of the Republic of Moldova is also to be amended to explicitly permit the Intelligence and Security Service of the Republic of Moldova to intercept computer data.[17] However, the Law Intelligence Service of the Republic of Moldova does not provide any limitations on the collection of data or judicial oversight.[18]

European Convention on Human Rights and will lead to arbitrary restrictions to receiving and imparting information, vital components of the freedom of expression.

[14] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 43, UN Doc. # A/HRC/17/27 (May 2011).

[15] Amendments, Article III(1).

[16] Amendments, Article VII(2).

[17] Amendments, Article I.

[18] *See*, The Law on the Intelligence Service of the Republic of Moldova, Articles 4, 8 and 9.

Analysis: The lack of judicial oversight is likely to lead or contribute to an impermissible restriction on the freedom of expression and right to privacy.[19] Surveillance, including targeted collection of data on specific individuals or communities directly interferes with the privacy and security necessary for freedom of opinion and expression.[20]

As currently drafted, the Amendments permit law enforcement officers (including Prosecutors and the Intelligence service) the power to compel data from computer users and internet service providers (ISPs) often without any judicial oversight. When judicial oversight is required in the Amendments, such judicial review is cursory with a low threshold, thus amounting to *de facto* approval, which may lead or contribute to an impermissible restriction on the freedom of expression.[21]

Although States may justify these types of interferences as being necessary to fight terrorism or maintain public order, such interferences are not necessary or proportionate in light of the specific threats to privacy and freedom of expression.[22] Under international law, States are called upon to "establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data."[23] The Amendments fail to meet Moldova's obligations to ensure that any surveillance of communications and interception or collection of personal data is made independently with real, effective judicial oversight.

Recommendation: The Amendments should be revised to require meaningful judicial oversight before the search, seizure, collection, storage or disclosure of electronic data.

No Protection for Whistleblowers or Journalists

Issue: The Amendments provide no protections for whistleblowers, journalists or other public watchdogs to carry out their work without facing criminal charges.

Analysis: The Amendments revise numerous provisions in the Criminal Code of the Republic of Moldova.[24] The damage elements to a number of crimes – "causing large scale damage" – are proposed to be removed. This will result in actions being criminalized even if no damage has occurred. For example, if the Amendments are passed, Article 259 of the Criminal Code of the Republic of Moldova, will criminalize mere "illegal access" to a computer or data storage device, even if no damage is caused.

---

[19] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 56, UN Doc. # A/HRC/23/40, (April 2013).
[20] David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 20, UN Doc. # A/71/373, (September 2016).
[21] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 56, UN Doc. # A/HRC/23/40, (April 2013).
[22] David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 20, UN Doc. # A/71/373, (September 2016).
[23] UN General Assembly, "Report of the Third Committee, The right to privacy in the digital age," page 2, UN Doc. # 68/456/ADD.2, (December 2013).
[24] *See*, Amendments, Article II.

Individually these articles[25] in the Amendments may appear to be reasonable changes necessary to uphold the integrity of computer systems and data. However, taken together, the Criminal Code of the Republic of Moldova may be used to stifle expression, suppress journalism and restrict access to information. Such actions, which will soon be criminalized, may often be necessary for journalists, whistleblowers, and other individuals and organizations monitoring the government. Although States should curtail and criminalize illegal surveillance, laws should not target whistleblowers or others seeking to expose human rights violations or provide legitimate oversight of government actions.[26] "States should recognize the importance of whistleblowers who act in the public interest to uncover human rights abuses and corruption in both the public and the private sector. They should adopt legislation and practices that afford whistleblowers protection and provide a safe alternative to silence."[27]

Recommendation: The proposed amendments to the Criminal Code of the Republic of Moldova be re-drafted to excuse such actions if they are undertaken in "good faith" and do not harm the underlying computer systems.[28]

Additional Concerns

The Amendments expand the requirement for all ISPs to keep records of all its users' data. ISPs must now keep records for all "prepaid" and "anonymous" services, as well as retain all data for at least six months.[29] These requirements amount to bulk compulsory data retention, which "greatly increase[s] the scope for infringement upon human rights," like the right to privacy.[30] Bulk compulsory data retention increases the scope of State surveillance, increases business expenses, which lowers profits, and increases the likelihood that the data will be stolen, accidentally disclosed or used to commit fraud.[31] The Amendments, and the underlying law – the Law on Preventing and Fighting Against Computer Crimes – should be revised to eliminate bulk compulsory data collection.

December 12, 2016

[25] The Criminal Code of the Republic of Moldova, Articles 259, 260^2, 260^3, 260^4, 260^6, and 261^1.
[26] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 84, UN Doc. # A/HRC/23/40, (April 2013).
[27] OSCE Office for Democratic Institutions and Human Rights (ODIHR), *Guidelines on the Protection of Human Rights Defenders*, p.10 (2014).
[28] *See* e.g., The UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, *Joint Declaration December 6, 2004*, p. 4 (2004).
[29] Amendments, Article VII(6).
[30] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 67, UN Doc. # A/HRC/23/40, (April 2013).
[31] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 67, UN Doc. # A/HRC/23/40, (April 2013).