Media Diversity Institute

THE RIGHT TO ONLINE ANONYMITY IN ARMENIA

Gevorg Hayrapetyan

YEREVAN
2023

THE RIGHT TO ONLINE ANONYMITY IN ARMENIA

Gevorg Hayrapetyan

CONTENTS

List of Abbreviations

RA	- Republic of Armenia
POPD Law	- Law “On Protection of Personal Data”
FOI Law	- Law “On Freedom of Information”
MC Law	- Law “On Mass Communication”
UN	- United Nations
CoE	- Council of Europe
ECHR	- European Court of Human Rights
CSO	- Civil Society Organization

Introduction

Everyone has the right to inviolability of his/her private and family life. This right, regardless of wording (right to privacy and family life, right to respect for private and family life, etc.),[1] as a fundamental human right, is reflected both in international legal acts and in the current and previous versions of the Constitution of the Republic of Armenia.[2]

The scientific-practical (doctrinal) interpretations of the 2020 version of the RA Constitution presented the content of a person's private life as follows: "(...) private life is the aspect of a person's privacy that they opt not to disclose to others due to their freedom. It is the part of a person's life that is untouchable by others. It reflects the innate desire of every person to have a private world of his/her intimate and business interests, without any interference. (...) The right to private life is the right of every person to express himself/herself and protect their identity."[3]

At the same time, as science and technology continue to advance, especially with the expansion of the Internet, human rights, including the right to privacy, are increasingly reflected in the online space, taking on new features, such as the access with no space and time limitations. The person's right to privacy on an online platform can manifest itself as, for example, a right to electronic privacy, a right to digital privacy, as well as a right to anonymity or a right to online anonymity.

The terms described above may to some extent vary in their meaning: for instance, the concept of the right to online privacy may consist of different elements depending on the specific terminology used. In one case, it may incorporate the inviolability of information of an identifiable (non-anonymous) person, while in other situations it may relate to the anonymity of the individual themselves.

The disclosure of an individual's identity and identification possibilities are directly related to personal data. In 2012, Armenia ratified the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Convention 108),[4] according to which, "personal data" means any information relating to an identified or identifiable individual ("data subject").[5] The same concept is preserved in the Protocol amending the CoE "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Convention 108+),[6] which was ratified by Armenia through the law that came into force on November 26, 2021.[7] In 2015, the RA Law "On Protection of Personal Data"[8] was adopted, according to which "personal data" shall mean any information relating to a natural person, which allows or may allow for direct or indirect identification of a person's

[1] In the current study, we will hereinafter mostly use the terms "privacy" or "inviolability of private life", given that the main focus of the paper will be on the right to privacy and opportunities to achieve it.

[2] Universal Declaration of Human Rights, Article 12, https://www.arlis.am/DocumentView.aspx?DocID=1896, International Covenant on Civic and Political Rights, Article 12, https://www.arlis.am/DocumentView.aspx?DocID=18500 Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8, https://www.arlis.am/DocumentView.aspx?DocID=81165

[3] Collection of Scientific-Practical Interpretations of the RA Constitution, 2020, pp. 276-277

[4] https://www.arlis.am/DocumentView.aspx?docid=81469

[5] https://www.arlis.am/DocumentView.aspx?docid=81469 CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 2

[6] http://www.parliament.am/draft_docs7/K-947lr_ardzanagrutyun.pdf

[7] https://www.arlis.am/DocumentView.aspx?DocID=157879

[8] https://www.arlis.am/DocumentView.aspx?DocID=175814

identity.[9] This notion of the POPD Law is essentially comparable to the notion of personal data enshrined in the Convention 108+.

At the same time, the Explanatory Report[10] of Convention 108+ states that data is to be considered as anonymous only as long as it is impossible to re-identify the data subject or if such re-identification would require unreasonable time, effort or resources, taking into consideration the available technology at the time of the processing and technological developments.[11]

"Anonymization" in the POPD Law is called "depersonalization" and is defined as operations, which render it impossible to identify the data that pertains to a specific data subject.[12]

In the context of the above-mentioned, the term "online anonymity" used within the scope of the current study refers to the ability of a person to appear in the online space without any information identifying him/her.

As a result, if summarized, the focus of this study is on examining the boundaries of an individual's ability to remain anonymous (unidentified) within the RA legislation, which, in its turn, is one of the manifestations of the right to privacy in the online space.

It should be noted that as a manifestation of an individual's right to privacy, online anonymity is closely related to another human conventional and constitutional right, namely the right to freedom of expression.[13] This is the right of everyone to freely express his/her opinion. This right includes freedom to hold own opinions, as well as to seek, receive, and impart information and ideas by any means of information without interference by state or local self-government bodies and regardless of state frontiers.[14] Online anonymity (like anonymity in general) serves as a guarantee of freedom of expression, and a lack of anonymity accordingly constrains freedom of expression.

In the context of all of the above, the core of this analytical paper is the claim deriving from the conventional and constitutional right to privacy that everyone has a right to online anonymity.[15]

[9] https://www.arlis.am/DocumentView.aspx?DocID=175814 RA Law "On Protection of Personal Data", Article 3, Paragraph 1.1

[10] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf , p. 15

[11] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf , p. 17, point 19

[12] https://www.arlis.am/DocumentView.aspx?DocID=175814 RA Law "On Protection of Personal Data", Article 3, Paragraph 1.9

[13] https://www.arlis.am/DocumentView.aspx?DocID=1896 Universal Declaration of Human Rights, Article 19, International Covenant on Civic and Political Rights, Article 19, https://www.arlis.am/DocumentView.aspx?DocID=18500
Convention for the Protection of Human Rights and Fundamental Freedoms, Article 10, https://www.arlis.am/DocumentView.aspx?DocID=81165

[14] RA Constitution, Article 42 https://www.arlis.am/DocumentView.aspx?DocID=143723

[15] The paper delves deeper in the examples of the recognition of this right and its boundaries in subsequent sections.

Examples of recognition of online anonymity in international law

The importance of online anonymity both from the perspective of privacy and freedom of expression has long been recognized. For instance, Article 19, an international organization that aims to propel freedom of speech/expression, including at the international level (the name of the organization is a reference to Article 19 of the Universal Declaration of Human Rights, which defines freedom of expression), developed a policy brief on the right to online anonymity in 2015, noting that the protection of anonymity is a vital component in protecting both the right to freedom of expression and the right to privacy.[16]

The issue of online anonymity has also become the subject of a report by the UN Special Rapporteur on Freedom of Expression and Opinion (A/HRC/29/32: Report on Encryption, Anonymity and the Human Rights Framework).[17] The report raises two key questions: first, do the rights to privacy and freedom of opinion and expression protect secure online communication, specifically by encryption or anonymity? And, second, assuming an affirmative answer, to what extent may Governments, in accordance with human rights law, impose restrictions on encryption and anonymity?[18] Through comparative analyses, the Special Rapporteur concluded that encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. The Special Rapporteur also noted that such security can be essential for the exercise of other rights.[19] Considering that because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective, the Special Rapporteur highlighted, among others, that states should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective.[20] The Special Rapporteur also found that states should promote encryption and anonymity, and national laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online.[21]

The Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights noted in one of his press releases that freedom of expression and privacy protect anonymous speech from government restrictions.[22]

---

[16] https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf , p. 1

[17] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

[18] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement, A/HRC/29/32, Report on Encryption, Anonymity and Human Rights Framework, p. 3, point 3

[19] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement, Report on Encryption, Anonymity and Human Rights Framework, p. 19, point 56

[20] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement, Report on Encryption, Anonymity and Human Rights Framework, p. 19, point 57

[21] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement, Report on Encryption, Anonymity and Human Rights Framework, p. 20, point 59

[22] https://www.oas.org/en/iachr/expression/showarticle.asp?artID=979&lID=1 , Press Release R17/15

There are regulations on anonymous interactions with the state in the CoE Convention "On Access to Official Documents",[23] which was ratified by Armenia through the law that came into effect on March 23, 2022.[24]

In particular, Part 2 of Article 4 of the Convention stipulates that the parties to the Convention may give applicants for information the right to remain anonymous except when disclosure of identity is essential in order to process the request.[25]

In Paragraph 42 of the official Explanatory Report on the Convention, with regards to Article 4, Part 2 of the Convention, it is highlighted that although this provision does not require Parties to the Convention to grant applicants a right to submit requests anonymously, it encourages this by including an optional obligation in this respect.[26]

The European Court of Human Rights has also addressed the right to online anonymity. In the "Standard Verlagsgesellschaft mbH v. Austria (no. 3)" Case Judgment[27], the ECHR found that the Austrian courts violated the applicant's right to freedom of expression by requiring the applicant to disclose the identity of the persons who had allegedly posted defamatory comments on the applicant's website.

The applicant was a Vienna-based company that published a daily newspaper both in print (Der Standard) and electronically (derStandard.at website). The applicant allowed website users to leave anonymous comments at the end of the pieces published online. At the same time, users provided their first name, last name, and e-mail address upon registration. Additionally, users could choose to provide their physical postal address, but they were informed that their data would not be publicly visible. On the other hand, users accepted the website's general terms and conditions, including the inadmissibility of insults, threats or abuse, as well as defamatory statements or statements damaging to businesses. The users were also notified that their data could be disclosed only if required to do so by law. The "Standard Verlagsgesellschaft mbH v. Austria (no. 3)" case centered around K.S. and H. K., protagonists of pieces published on derStandard.at, who in 2012 and 2013, considering that some of the comments on the mentioned pieces contained defamation against them, requested the media to disclose the identity of the comments' authors in order to file an appropriate lawsuit against them. Although the Austrian courts initially rejected K.S. and H. K.'s request, the media was eventually obligated to disclose the identities of the commenters after an appeal.

As a result, the issue of the disclosure of the news website commenters' identities was taken up by the ECHR. The ECHR Judgment on "Standard Verlagsgesellschaft mbH v. Austria (no. 3)" case may trigger debates about the right to freedom of expression under Article 10 of the European Convention on Human Rights, which is somewhat beyond the scope of the current study. Nevertheless, it is important that the ECHR's decision, in fact, acknowledged the importance of online anonymity in the context of freedom of expression.

It is also noteworthy that although the applicant was a media company, the ECHR did not consider the lack of justification for the disclosure of the commenters' identities in the context of the confidentiality of the (journalistic) source of information: thus, the ECHR did not view

[23] http://www.parliament.am/law_docs_8/280322HO68_konventcia.pdf
[24] https://www.arlis.am/DocumentView.aspx?DocID=161489
[25] http://www.parliament.am/law_docs_8/280322HO68_konventcia.pdf , p. 5, Article 4, Part 2
[26] Council of Europe Convention on Access to Official Documents, Explanatory Report, http://www.foi.am/u_files/file/legislation/EuropeConventioneng.pdf, p. 7, Paragraph 42
[27] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-213914%22]}

the authors of online comments as journalistic sources, while it found the Austrian courts' decisions to oblige the applicant to disclose the identities of its anonymous commenters to be unfounded. The ECHR also noted that there is no absolute right to anonymity, which albeit an important value, should be balanced against other rights and interests.

Based on the above-mentioned, the following conclusions can be drawn, which will be pertinent to the current study:

- the right to anonymity is a manifestation of the fundamental right to privacy and a guarantee of the fundamental right to freedom of expression. The interference with the right to anonymity may lead to the violation of the right to privacy and have a chilling effect on free expression;

- the right to privacy and freedom of expression are fundamental, universal rights;

- respect for the right to privacy and freedom of expression and the right to anonymity that stems from them and their provision must be upheld regardless of the context, including online;

- any restrictions on the right to online anonymity must comply with the principles of legality, necessity, proportionality and legitimacy.

Purpose

The purpose of this study can be better defined by answering the following questions:

- what - as we mentioned above, the focus of this analysis is the boundaries of an individual's ability to remain anonymous (unidentified) within the RA legislation, hence in this case anonymity in the online space needs to be discussed;

- whom - in this case the focus is on an individual - physical persons, people. Nevertheless, it is important to bear in mind that Article 74 of the RA Constitution envisages that the basic rights and freedoms shall also extend to legal persons to the extent these rights and freedoms, by virtue of their nature, are applicable thereto;

- from whom - as part of the current study, it is crucial to address the issue of a person's ability to remain anonymous (unidentified) in the online space vis-à-vis the state, in a broad sense - the institutions and officials envisaged by the Constitution and laws, including the organizations and persons through which state institutions can exercise their governmental powers.

Thus, the current study seeks to examine the state of the right to anonymity in the online space in Armenia, including the boundaries of a person's ability to remain anonymous (unidentified by the state) and to provide appropriate recommendations based on the identified problems.

Methodology

Given the purpose of the current paper, a study of domestic legislation was carried out in order to determine the state of the right to anonymity in the online space in Armenia, including the boundaries of a person's ability to remain anonymous (unidentified by the state).

Moreover, first, the analysis focused on studying the existence of general regulations (defining or excluding) related to the right to online anonymity. This implies the possibilities of avoiding constant and basically unlimited surveillance of the state not in specific legal relationships, but in the online space in general, regardless of whether it is possible to ensure anonymity in individual cases or not.

The next step of the analysis involved examining examples of regulations related to the right to anonymity in specific legal relationships, encompassing both the current legislation and legislative initiatives that have not been adopted.

The search for online anonymity regulations in the legislation was conducted using a basic (without employing specialized software) search methodology. In particular, the necessary information was searched within the Armenian Legal Information System (arlis.am or laws.am) in such legal acts and through such keywords that could be reasonably related to the right to online anonymity (for example, the following terms in multiple declensions were searched: "anonymous", "anonymity", "private life", "privacy", "freedom of information" and other similar words).

The study analyzed separately the general regulations related to privacy and freedom of information rights: legal documents such as the Constitution, the Civil and Criminal Codes, the Laws "On Protection of Personal Data" and "On Freedom of Information" were examined. Based on the analysis of these legal acts, a relevant conclusion was drawn regarding the presence/absence of a general regulation of the right to online anonymity.

The study analyzed sectoral laws that in some way relate to the right to anonymity. In particular, the Criminal Procedure Code, the Law "On Electronic Communications", the Law "On Mass Communication" and the Law "On Whistleblowing System" were all presented separately in the study. Based on the analysis of these legal acts, relevant conclusions were also drawn regarding the appropriateness of specific regulations of the right to online anonymity.

The study's conclusions contain solely substantive assessments. Based on the conclusions, the study presents recommendations on the identified problems addressed to the government, the legislative (deputies) and civil society.

Along with legal regulations, the relevant judicial and administrative practice was also presented in the study.

International best practice served as a guideline for the current study, in particular, the key takeaways from that practice, which were presented at the end of "Examples of online anonymity recognition in international law" section.

Current state

Prior to addressing the problems associated with the right to anonymity and suggesting ways to tackle them, it is necessary to first have a comprehensive understanding of the legal and practical regulations of online anonymity, and its current state.

The study's Introduction and "Examples of online anonymity recognition in international law" section have already outlined the main international documents ratified by Armenia, which enshrine the rights to privacy and freedom of expression, and acknowledge the right to online anonymity. Therefore, this section of the study will not separately present these documents but rather refer to them as necessary.

General Regulations

There is no separate law in Armenia regulating people's online behavior, including one specifically establishing the right to online anonymity. As a result, in order to evaluate the presence or absence of the right to online anonymity, it is necessary to refer to the general regulations related to the rights to privacy and freedom of information. These, in particular, are:

Constitution[28]

The RA Constitution enshrines both the right to the inviolability of a person's private life and the freedom of expression, while also defining the restrictions of these rights (mandatory conditions, principles for the application of a right's restriction).

Thus, according to Article 31 of the Constitution: "1. Everyone shall have the right to inviolability of his or her private and family life, honor and good reputation. 2. The right to inviolability of private and family life may be restricted only by law, for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others."

According to Article 33 of the Constitution: "1. Everyone shall have the right to freedom and secrecy of correspondence, telephone conversations and other means of communication. 2. Freedom and secrecy of communication may be restricted only by law, for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others. 3. The secrecy of communication may be restricted only upon court decision, except where it is necessary for the protection of state security and is conditioned by the particular status of communicators prescribed by law."

According to Article 34 of the Constitution: "1. Everyone shall have the right to protection of data concerning him or her. 2. The processing of personal data shall be carried out in good faith, for the purpose prescribed by law, with the consent of the person concerned or without such consent in case there exists another legitimate ground prescribed by law. (…) 5. Details related to the protection of personal data shall be prescribed by law."

[28] https://www.arlis.am/DocumentView.aspx?DocID=143723 , Articles 31, 33, 42 and 78

According to Article 42 of the Constitution: "1. Everyone shall have the right to freely express his or her opinion. This right shall include freedom to hold own opinion, as well as to seek, receive and disseminate information and ideas through any media, without the interference of state or local self-government bodies and regardless of state frontiers. (...) 3. Freedom of expression of opinion may be restricted only by law, for the purpose of state security, protecting public order, health and morals or the honor and good reputation of others and other basic rights and freedoms thereof."

Article 78 of the Constitution defines the principle of proportionality, according to which: "The means chosen for restricting basic rights and freedoms must be suitable and necessary to achieve the objective prescribed by the Constitution. The means chosen for restriction must be proportionate to the significance of the basic right or freedom being restricted."

Civil Code[29]

The RA Civil Code defines privacy as a non-material value[30] and grants a person the legal entitlement to seek compensation for the non-material damage suffered, if a person can prove that as a result of the decision, action or inaction of a state or local self-government body or its official, the rights of that person have been violated, including the right to respect for private life.[31]

In the RA Civil Code, anonymity is referenced only in the context of copyright (in the provisions on anonymous works).

The document does not address any other type of anonymity, including online anonymity.

Criminal Code[32]

The RA Criminal Code stipulates liability for the use, exploitation or disclosure of information constituting personal or family secret of a person without his/her consent, or acquisition or storage of that information with the aim of using, exploiting or disclosing it in violation of the manner established by law.[33]

A separate chapter of the Criminal Code deals with crimes against computer system and computer data security.[34] In this case, however, the focus is mainly on cybercrimes.

The RA Criminal Code does not address any other type of anonymity, including online anonymity.

[29] https://www.arlis.am/DocumentView.aspx?DocID=172116
[30] https://www.arlis.am/DocumentView.aspx?DocID=172116, RA Civil Code, Article 162
[31] https://www.arlis.am/DocumentView.aspx?DocID=172116, RA Civil Code, Article 162.1
[32] https://www.arlis.am/DocumentView.aspx?DocID=176079
[33] https://www.arlis.am/DocumentView.aspx?DocID=176079, RA Criminal Code, Article 204
[34] https://www.arlis.am/DocumentView.aspx?DocID=176079, RA Criminal Code, Chapter 38, Articles 359-365

Law "On Protection of Personal Data"[35]

The POPD Law regulates the procedure and conditions for processing personal data, exercising state control over them by state administration or local self-government bodies, state or community institutions or organizations, legal or natural persons.[36] As a general legal act regulating the processing of personal data, the POPD Law does not prohibit the processing of certain personal data, including its publication, nor does it classify certain personal data as confidential. This viewpoint was expressed by the authorized body for personal data protection, operating on the basis of the POPD Law (Agency for Protection of Personal Data) in its decision on the administrative case N-006/01/19. In the same decision, the POPD authorized body noted that the laws regulating certain relations or the activities of a specific body or a specific legal relationship may directly determine whether particular personal data can be transferred (as well as published) or not.[37]

As noted in the introduction of this study, "anonymization" in the POPD Law is called "depersonalization"[38], but the POPD Law presents the depersonalization of personal data as a component of the principle of proportionality of personal data processing: thus, the POPD Law prohibits the data processor from processing personal data if the purpose of data processing is possible to achieve in a depersonalized manner.[39]

While the POPD Law does not directly address online anonymity, it considers any operation involving personal data to be personal data processing, irrespective of the format and manner of implementation, including automated processing. Additionally, according to the same document, the transfer of personal data to third parties encompasses, among others, posting personal data on information communication networks or otherwise making personal data available to another person.[40]

Law "On Freedom of Information"[41]

Freedom of information, namely the right to seek, receive and disseminate information, is an integral part of the freedom of expression. The Law "On Freedom of Information", which has been in force in Armenia since 2003, regulates relations pertaining to freedom of information and, among other things, establishes the procedure, formats and conditions for receiving information.

The FOI Law envisages the procedure and conditions for providing information both proactively (at the initiative of the information holder) and in response to a request by the person seeking information. However, submitting anonymous requests for information, is not envisaged under this law. In particular, the FOI Law stipulates that anyone seeking information must submit a signed, written request that includes the applicant's name, surname, citizenship, place of residence, work or study.[42] Moreover, if any of the above data

---

35 https://www.arlis.am/DocumentView.aspx?DocID=175814
36 https://www.arlis.am/DocumentView.aspx?DocID=175814, RA Law "On Protection of Personal Data", Article 1
37 http://www.foi.am/u_files/file/Voroshum_2019_qaghaqapetaran.pdf, pp. 9-10, Point 46
38 See page 5 of the study
39 https://www.arlis.am/DocumentView.aspx?DocID=175814, RA Law "On Protection of Personal Data", Article 5, Paragraph 4
40 https://www.arlis.am/DocumentView.aspx?DocID=175814, RA Law "On Protection of Personal Data", Article 3, Part 1, Paragraphs 1, 2 and 3
41 https://www.arlis.am/DocumentView.aspx?DocID=175858
42 https://www.arlis.am/DocumentView.aspx?DocID=175858, RA Law "On Freedom of Information", Article 9, Part 1

is missing, the written request is disregarded (i.e., the written request may, in fact, be left without a response).[43]

Requests for receiving information can also be submitted online through e-request.am, a unified portal for online requests.[44] This platform allows submitting unsigned requests. However, to do that, it is necessary to first register on the platform, by providing personal information such as name, surname, date of birth, passport data, e-mail and phone number. As a result, even if the applicant submits an unsigned request, not only his/her name, surname, citizenship and address, as defined by the FOI Law, but also the phone number and e-mail are automatically displayed in the online request.

The inability to submit anonymous requests under the FOI Law has been a recurring concern for civil society. In particular, back in 2016, CSOs were engaged in the development of a concept of modernization for the freedom of information sector, in which, among others, they raised the issue of ensuring everyone's right to submit a request. In that context, the concept argued that the FOI Law provision on information about the applicant submitting a request was an unnecessary formality for individuals exercising their rights in the field of ensuring freedom of information.[45] As a solution, the concept suggested removing the citizenship and signature elements from the list of mandatory requirements for a request. As a result, the concept and the FOI Law reforms that came alongside with it, were not adopted, due to a lack of consensus between the civil society and state bodies on the modernized version of the Law.

In 2020 as well, the issue of the inability to submit anonymous requests under the FOI Law was discussed at the proposal of civil society organizations.[46] As a result, the RA Ministry of Justice developed a draft amendment to the FOI Law, where it was proposed to establish in the FOI Law that only the name and surname of the applicant, as well as the postal or e-mail addresses should be mentioned in the written request.[47] This time, among other things, this amendment to the FOI Law was backed[48] by the CoE Convention "On Access to Official Documents", which encourages the establishement of a possibility of submitting anonymous requests. According to the proposed changes, the requirement of specifying name and surname in the request, in situations when information on citizenship, signature and addresses of residence, work or study was not required, would have exclusively served the purpose of ensuring appropriate correspondence (ethics of correspondence) with the applicant, without even giving the information holder an opportunity to verify, if necessary, the authenticity of the name and surname provided by them. This initiative aimed at ensuring anonymity in the field of freedom of information was not completed either.[49]

---

[43] https://www.arlis.am/DocumentView.aspx?DocID=175858, RA Law "On Freedom of Information", Article 9, Part 3

[44] https://e-request.am/en

[45] https://www.moj.am/legal/view/article/969, Concept on Modernization of Freedom of Information Sector, Part 2, Paragraph 2

[46] Freedom of Information Center NGO, Committee to Protect Freedom of Expression NGO

[47] https://www.e-draft.am/projects/2489/about, Draft Amendments to the RA Law "On Freedom of Information"

[48] https://www.e-draft.am/projects/2489/justification, Justification of the draft amendments to the RA Law "On Freedom of Information" (the CoE Convention "On Access to Official Documents" was in the process of signing and ratification by Armenia at that time)

[49] There was no official clarification by the RA Ministry of Justice, which developed the draft, but presumably the reason for suspending the adoption of the draft was the challenges faced by Armenia due to the coronavirus pandemic and the 44-Day War in 2020.

Conclusion

- As noted, there is no specific law directly defining the right to online anonymity in Armenia. The country's general legal acts related to the rights to privacy and freedom of expression do not explicitly define online anonymity (under such a term) either. At the same time, the RA Constitution does not condition the exercise of the rights to privacy and freedom of expression to a specific platform, i.e., space or place.

  As a result, the RA legislation generally does not limit a person's ability of avoiding constant and basically unlimited state surveillance in the online space, regardless of whether anonymity is possible in individual cases or not. Despite the lack of explicit definition to the right to online anonymity in the RA Constitution, as well as the international treaties cited in this study, within the jurisdiction of the RA Constitution and, accordingly, other legal acts related to the rights to privacy and freedom of expression, everyone enjoys both of the rights, including the right to anonymity (also online) stemming from them. **Hence, in the context of the right to inviolability of private life, everyone has the right to online anonymity, which can only be restricted by the law, provided that such restrictions comply with the constitution's purposes and the principle of proportionality.**

- As a guarantee of freedom of expression, the right to act anonymously in the context of freedom of information is not properly addressed in the RA Law "On Freedom of Information", the requirements for information requests under the FOI Law do not reflect the international best practices on the right to anonymity.

Examples of Specific Regulation

Despite the lack of a separate law in Armenia that explicitly defines or excludes the right to online anonymity, there are specific examples when sectoral laws guarantee or, on the contrary, restrict the possibility of online anonymity.

Law "On Electronic Communications"[50]

Online anonymity and the ability to ensure the inviolability of private life in the online space largely depend on various online service[51] providers that process customers' personal data within their respective services, as well as electronic communication service providers that deal with customers' personal data in the context of providing electronic communication service, including Internet service. It is noteworthy that in order to use various services in the online space, it is necessary to first obtain an electronic communication service, in particular, an Internet service. Moreover, while the processing of personal data in various online relationships is based only on the service recipient's (data subject's) consent (the service provider-customer contract, privacy policy, terms and conditions, terms and references of service provision, online platform use, etc.), electronic communication,

[50] https://www.arlis.am/DocumentView.aspx?DocID=172158

[51] The term "online services" does not only refer to a service or product offerings. Instead, the term encompasses a wide range of online services designed to satisfy human needs such as physiological needs, leisure, entertainment, social interaction, scientific, literary, artistic, informational needs, interests and curiosity-based needs, etc. In other words, anything offered online apart from electronic communications (Internet) service that is originally made available for online use, falls under the category of "online service".

including Internet services, are also subject to legal regulations in addition to the customer-service provider contract.

Thus, the Law "On Electronic Communications" considers any person using or requesting public electronic communication services to be a customer or subscriber, except for those who offer or provide telecommunication services.[52]

In the context of the above, it is crucial that, on the one hand, the electronic communication service does not include services providing or exercising editorial control over the content transmitted via electronic communication networks.[53] On the other hand, Article 49 of the Law "On Electronic Communications" defines the confidentiality of customer information, emphasizing, among others, that each operator and service provider shall be obliged to treat and keep as confidential the information regarding the type, location, purpose, destination, quantity, technical conditions of services used by its customers.[54]

The Law "On Electronic Communications" also stipulates that any person other than a party to a message transmitted by any electronic communication means may intercept, record or disclose the content of such message only upon the written consent of the parties to the message or upon a court decision in cases and in the manner provided for by law.[55]

Criminal Procedure Code[56]

The right to online anonymity, as a manifestation of the right to inviolability of private life, may only be restricted by law, for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others. The task of ensuring the stated objectives is often comparable to the functions of law enforcement agencies.

On July 1, 2022, the RA new Criminal Procedure Code entered into force, with the aim of establishing an efficient procedure for the conduct of proceedings in relation to alleged crimes, based on securing the rights and freedoms of a person.[57]

Article 26 of the Criminal Procedure Code separately addresses the issue of a person's private and family life, outlining, among other things, that the competent authorities may collect, store and use information about a person without his/her consent only in the cases and manner provided by law, if it is necessary to uncover circumstances relevant to the proceedings. Additionally, the article specifies that interference with a person's correspondence, telephone conversations and other forms of communication during the proceedings can be carried out solely via a court decision, in the cases and manner provided by law. Article 26 also emphasizes that during the proceedings, the information relating to a person and containing medical (with the exception of data related to seeking or receiving

[52] https://www.arlis.am/DocumentView.aspx?DocID=172158, RA Law "On Electronic Communications", Article 2
[53] https://www.arlis.am/DocumentView.aspx?DocID=172158, RA Law "On Electronic Communications", Article 2
[54] https://www.arlis.am/DocumentView.aspx?DocID=172158, RA Law "On Electronic Communications", Article 49
[55] https://www.arlis.am/DocumentView.aspx?DocID=172158, RA Law "On Electronic Communications", Article 50, Paragraph 1
[56] https://www.arlis.am/DocumentView.aspx?DocID=176081
[57] https://www.arlis.am/DocumentView.aspx?DocID=176081, RA Criminal Procedure Code, Article 2

medical assistance and services), notarial, banking or correlated secrets may only be collected via a court decision, in the cases and manner provided by law.[58]

Article 232 of the Criminal Procedure Code, in its turn, lays out the procedure for investigators to request information in writing from state or local self-government bodies, legal entities or any other organization possessing information about circumstances relevant to the proceedings. The Code stipulates that the request for information is mandatory for the addressee, except for certain cases, including when the requested information is confidential under the law. The same article entitles the investigator to request, with a decision approved by the supervising prosecutor, the following:

- the phone numbers of those who communicate through fixed or mobile phone network, data about an individual associated with the subscriber of the phone number;[59]

- the data necessary to identify the location of the communicators and their movement at the time of starting the telephone communication and during it;

- the place, time and duration of Internet connection and disconnection, the identification data of the Internet user or subscriber, the telephone number used to connect to the public telephone network, the Internet address, including the Internet Protocol (IP) address, the identification data of the recipient of the Internet telephone call.

Article 232 of the Code stipulates that the above-mentioned data may be requested in relation to a natural person, when there is evidence suggesting his/her commission of an alleged crime. The provision is also applicable to the accused, the victim or the witness, if it is necessary to verify the testimony thereof.[60]

A comparison of Articles 26 and 232 of the Criminal Procedure Code shows that the document attempted to distinguish between privacy-intrusive information and other non-privacy-encumbered information about a person. In compliance with international best practices, higher standards were set for obtaining privacy-intrusive information such as, among others, a court decision, while for other non-privacy-encumbered information about a person, lower standards of intervention were set, namely a written request from an investigator or an investigator decision approved by the supervising prosecutor.

Nevertheless, Article 232 of the Criminal Procedure Code has sparked certain concerns within civil society and especially information security professionals in terms of illegitimate or disproportionate interference with the privacy of a person, including freedom of communication and online anonymity, carried out without judicial oversight. Such concerns were often conveyed through individual posts or comments.

The problematic nature of Article 232 of the Criminal Procedure Code has also been addressed by the authorized body for the protection of personal data.

In general, concerns surrounding Article 232 can be classified into the following points:

- It is alarming that Article 232 of the Criminal Procedure Code uses outdated terminology, such as “data about an individual” and “identification data” mentioned in

[58] https://www.arlis.am/DocumentView.aspx?DocID=176081, RA Criminal Procedure Code, Article 26, Parts 1, 4 and 5
[59] The term “data about an individual” is used in Article 232 of the RA Criminal Procedure Code
[60] https://www.arlis.am/DocumentView.aspx?DocID=176081, RA Criminal Procedure Code, Article 232

Article 232. Instead, the data relating to a natural person and directly or indirectly identifying him/her is recognized as “personal data” and is included in Article 34 of the 2015 edited RA Constitution and in the RA Law “On Protection of Personal Data” adopted in 2015. While this may appear a formal/technical issue at first glance, however, given that the new Criminal Procedure Code came into effect in 2022, i.e., 7 years after the adoption of the 2015 edition of the RA Constitution and the POPD Law, the use of such old terminology in the Code indicates that that Article 232 has not taken into account the developments in the right to privacy, online anonymity and international best practices in the online space.

- According to part 3 of the Criminal Procedure Code Article 232: “3. By the decision of the investigator approved by the supervising prosecutor, the following data may be requested: 1) the phone numbers of those who communicate through fixed or mobile phone network, data about an individual associated with the subscriber of the phone number; (…) 3) the place, time and duration of Internet connection and disconnection, the identification data of the Internet user or subscriber, the telephone number used to connect to the public telephone network, the Internet address, including the Internet Protocol (IP) address, the identification data of the recipient of the Internet telephone call.”

The study has already addressed Article 49 of the RA Law “On Electronic Communications”, where in part 1 it is stipulated that “1. Each operator and service provider shall be obliged to treat and keep as confidential the information regarding the type, location, purpose, destination, quantity, technical conditions of services used by its customers.” Consequently, “the data about an individual associated the subscriber of the phone number”, as well as “the place, time and duration of Internet connection and disconnection, the identification data of the Internet user or subscriber”, “the identification data of the recipient of the Internet telephone call” mentioned in parts 1 and 3 of Article 232 of the Criminal Procedure Code constitute confidential information under Article 49 of the RA Law “On Electronic Communications”. This indicates that investigators may obtain, among others, confidential information.

Here again reference should be made to Article 26 of the Criminal Procedure Code, where in part 5 it is emphasized that “ during the proceedings, the information relating to a person and containing medical, notarial, banking or correlated secrets may only be collected via a court decision, in the cases and manner provided by law”.

As a result, on the one hand, Article 26 of the Criminal Procedure Code makes it mandatory to have a court decision for obtaining confidential information, and on the other hand, in fact, a relevant court decision is not a prerequisite for obtaining the information defined as relating to a person by Article 232, part 3, points 1 and 3 of the Criminal Procedure Code and confidential by Article 49 of the RA Law “On Electronic Communications”.

It turns out, thus, that two different articles of the Code set different requirements for collecting (receiving) commensurate (with a similar status and regime) information.

Pursuant to Article 232, part 3, point 3 of the Criminal Procedure Code, an investigator may also request and obtain the “Internet address, including the Internet Protocol (IP) address” of the subscriber with a decision approved by the supervising prosecutor.

An Internet address includes both an Internet Protocol (IP) address and a Uniform Resource Locator (URL) or Internet domain name.

In this regard, it should be noted that a person's online behavior can be disclosed not only through the Internet content itself, but also through their Internet address, at least to a certain extent, as long as it contains links to the websites they have visited, which can reveal the Internet content they accessed. In such conditions, the Internet address, in fact, falls under the scope of the inviolability of a person's private life, as well as the right to freedom and privacy of correspondence, telephone conversations and other forms of communication, which can be interfered with only via a court decision (part 3 of Article 33 of the RA Constitution, part 4 of Article 26 of the RA Criminal Procedure Code, part 1 of Article 50 of RA Law "On Electronic Communications").

Law "On Whistleblowing System"[61]

There are also legislative regulations aimed at securing online anonymity rather than restricting it.

In 2018, the Law "On the Whistleblowing System" came into effect, which regulates the relationships associated with whistleblowing, the procedure for whistleblowing, the whistleblowers' rights, the responsibilities of state and local self-government bodies and organizations with regards to whistleblowing, as well as the protection of whistleblowers and their related persons.

The Law "On Whistleblowing System" addresses a range of issues, including ensuring the whistleblowers' anonymity. In particular, the law permits whistleblowers to anonymously report instances of corruption or conflicts of interest or violations of codes of conduct, incompatibility requirements or other restrictions or violations related to asset declaration, by using a unified electronic whistleblowing platform (Azdararir.am). At the same time, the law stipulates that through the unified electronic platform, the Republic of Armenia, represented by an authorized body of the Government of the Republic of Armenia, guarantees the protection of whistleblowers by ensuring their anonymity. According to the law, the whistleblowers' anonymity is ensured via the unified electronic platform through the encryption of their Internet Protocol addresses.[62]

According to the Law "On Whistleblowing System", whistleblowers should submit the anonymous report through a unified electronic platform.[63] The law also ensures that when filing an anonymous report, the whistleblowers' personal data will not be disclosed either to the competent authority or to other parties, except for the cases when whistleblowers disclose their personal data. At the same time, the law prohibits the competent authority from taking measures to reveal the personal data of the whistleblower who submitted an anonymous report.[64]

Apparently, the Law "On Whistleblowing System" establishes the possibility to remain anonymous only when whistleblowing online through the electronic platform. The Law also requires the competent authority to refrain from taking any measure to eliminate the whistleblowers' online anonymity and reveal their identity. Based on this provision of the

[61] https://www.arlis.am/DocumentView.aspx?DocID=172131
[62] https://www.arlis.am/DocumentView.aspx?DocID=172131, RA Law "On Whistleblowing System", Article 8, Paragraphs 1, 2 and 3
[63] https://www.arlis.am/DocumentView.aspx?DocID=172131, RA Law "On Whistleblowing System", Article 9, Paragraphs 1
[64] https://www.arlis.am/DocumentView.aspx?DocID=172131, RA Law "On Whistleblowing System", Article 11

Law, in case of online whistleblowing through the unified electronic platform, taking measures to reveal the whistleblowers online identities will be illegitimate by itself.

RA Law "On Mass Communication"[65]

The "Examples of online anonymity recognition in international law" section of the current study discussed the decision made in "Standard Verlagsgesellschaft mbH v. Austria (no. 3) case", by which the ECHR did not consider the anonymity of the authors of online comments as confidentiality of a journalistic source, neither did it recognize the individuals who left anonymous comments online as journalistic sources.

In 2021, the RA National Assembly put forward a draft law[66] that proposed amendments and supplements to the RA Law "On Mass Communication". One of the proposed changes was to define the concept of an anonymous source as a domain registered on the Internet, a website with hosting, or a user account or channel of an Internet site or application whose administrator's identification information is hidden from the reader. Added to that, as a restriction to the right to freedom of speech in reporting, the draft law proposed prohibiting references to anonymous sources (except for the cases specified by Article 9, part 2 of the Law "On Mass Communication").

The draft law came under criticism and in the same year was replaced by another document,[67] which proposed to define the concept of an "unidentifiable source" as a domain registered on the Internet, a website with hosting, or an account, channel or page (source) of a website or application whose administrator's identification information was absent or apparently false, provided that such defficiency hindered the identification of the administrator of the source. Among other things, the new draft stipulated that the administrator's identification information were the name, surname, residence or registration address of the natural person who administrated the source, if he/she carried out media activity as a private entrepreneur, as well as the state registration number. The new draft replaced the ban[68] on referring to anonymous sources and envisaged liability for media activity operators for the dissemination of information, if it was a reproduction of information disseminated by an unidentifiable source, irrespective of whether they referred to the latter. The new draft amending and supplementing the Law "On Mass Communication" was adopted and entered into force on January 1, 2022.[69]

Accordingly, the MC Law currently includes the concept of an unidentifiable source, along with a list of source identification data[70]. Additionally, the law stipulates that media cannot avoid liability for disseminating information in case reference is made to an unidentifiable source.[71]

As noted above, the initial draft proposing amendments and supplements to the Law "On Mass Communication" was revised due to criticism. It is noteworthy that the ban on referring to anonymous sources was removed from the new draft, and the substituting provision of

---

[65] https://www.arlis.am/DocumentView.aspx?DocID=164454
[66] http://www.parliament.am/drafts.php?sel=showdraft&DraftID=60991
[67] http://www.parliament.am/legislation.php?sel=show&ID=7863&lang=arm
[68] Which, by the way, envisaged administrative liability
[69] https://www.arlis.am/DocumentView.aspx?docid=159043
[70] https://www.arlis.am/DocumentView.aspx?DocID=164454, RA Law "On Mass Communication", Article 3, Part 1, Point 5
[71] https://www.arlis.am/DocumentView.aspx?DocID=164454, RA Law "On Mass Communication", Article 9, Part 2, Point 3

not releasing the media from liability for disseminating information in case reference is made to an unidentifiable source was more in line with the legal practice established at that time. Thus, mechanisms to protect oneself against the dissemination of information through media by a source of information or author acting anonymously or with false data had been developed within the framework of judicial precedents related to Article 1087.1 of the RA Civil Code, which provides for liability for insult and defamation. According to Article 1087.1, when the source of information or the author acts anonymously or with false data, the "disseminator" of that information (in other words, the publisher, reprinter or reproducer) is the party responsible for the interference of that information.[72] The Court of Cassation provided a detailed interpretation of the term "source of information" in its rulings No. EKD/2293/02/10 and No. LD/0749/02/10. The Court of Cassation established criteria to determine the legitimacy of a "source", based on which natural or legal persons with anonymous or false data (for example, anonymous users in social networks or on the Internet in general) are not legitimate "sources" either.[73]

As for the concept of an anonymous source, the replacement of the term "anonymous source" with "unidentifiable source" and introduction of a list of source identification data have not eliminated the concerns related to those provisions of the MC Law.

In particular, the MC Law considers an unidentifiable source to be a domain registered on the Internet, a website with hosting, or a user account, channel or page of a website or application, whose administrator's identification information is absent or apparently false or incomplete, provided that such defficiency hinders the identification of the administrator of the source. At the same time, source identification information are the name, surname, residence or registration address in the case of a natural person who administers the source.

In other words, the Law "On Mass Communication" finds the name, surname and address of a natural person to be sufficient to claim that the user and, accordingly, the source is not anonymous. In this regard, it should be noted that the scope of the identification information required to verify the administrator of the source is such that neither the readers, nor the media nor journalists will have and will be able to have such a database with which they would be able to determine the authenticity of the user's name and surname, or the accuracy of the address provided by him/her. Consequently, it turns out that any user on the Internet with an account containing any name, surname and address, will be recognized as an identified source under the MC Law, whereas those who use fake names, surnames and addresses actually appear to be acting anonymously online and remain practically unidentified.

Conclusion

- The sectoral laws that guarantee or restrict the possibility of online anonymity in Armenia may contain regulations that align with international best practices, as well as regulations that contradict them. Sectoral laws restricting the right to online anonymity pose a particular challenge: they often fail to take into consideration the developments in the field of privacy and freedom of expression, including the right to online anonymity. These laws fail to properly evaluate the impact and proportionality of the

[72] https://www.osce.org/files/f/documents/2/e/123447.pdf , Information Disputes Council "Defamation an Insult: A Guide for Journalists and Lawyers" by Ara Ghazaryan, Artak Zeynalyan, p. 13, Yerevan, 2014
[73] https://www.osce.org/files/f/documents/2/e/123447.pdf , Information Disputes Council "Defamation an Insult: A Guide for Journalists and Lawyers" by Ara Ghazaryan, Artak Zeynalyan, pages 42, 43, Yerevan, 2014

restriction of the right to anonymity in terms of interference with the rights of privacy and freedom of expression.

- Article 232 of the Criminal Procedure Code is problematic, leading to misunderstanding and misinterpretation. It seems to have been drafted in the early stages of the development of the new Criminal Procedure Code and not to have been reviewed, updated or aligned with the regulations of other laws in the field when being adopted.

- The provisions of the MC Law regarding the concept of an unidentifiable source and the list of identification information of the source administrator are problematic. These provisions are clearly inadequate in regulating and ensuring the accuracy and reliability of the news/information source, resulting, thus, in comments and confusion that run contrary to online anonymity (as a phenomenon).

Recommendations

- There is no need for a separate law regulating the right to online anonymity and its restrictions. The rights to inviolability of private life and freedom of expression enshrined in the international treaties ratified by the RA and the RA Constitution are sufficient to properly ensure the right to online anonymity.

- The rights to privacy and freedom of expression in the online space, including the right to online anonymity, should be guaranteed in the same way as they are in the physical world. And the state is limited in its ability to restrict the rights to inviolability of private life and freedom of expression in the online space, including the right to online anonymity, to the same extent as it is in the physical world.

- The state (the Government and the National Assembly) should ensure the compliance of new legal acts in a certain way relating to/restricting human rights in the online space with the rights to inviolability of private life and freedom of expression. Meanwhile, existing legal acts should be evaluated from the perspective of these fundamental rights and revised as necessary.

- It is necessary to resume the review of the requirements for written requests to receive information under the RA Law “On Freedom of Information” and exclude from the list the requirements to provide information about citizenship, signature, and specific address of residence, work or study, as well as to ensure the legal grounds and practical means to submit requests anonymously.

- It is necessary to revise Article 232 of the Criminal Procedure Code, exclude from the list of information in Part 3 of Article 232 confidential data such as information restricting the right to inviolability of private life, including the Internet address. Instead, it is proposed to establish that the collection of such information during the proceedings should only be authorized via a court decision. In addition, it is necessary to align the terminology of Article 232 of the Criminal Procedure Code with that of the Constitution and the Law “On Protection of Personal Data”.

- It is recommended to remove from the MC Law the provisions related to the concept of an unidentifiable source and the list of identification information of the administrator of the source. Thus, in compliance with judicial practice and international best practices, it is advised to review the provision (formulation) on non-exemption of the media from liability for disseminating information in case of reference to an unidentified source.