# The digital (il)literacy of local and regional politicians and civil servants – An analysis based on recent data from Romania

Robert MÜLLER-TÖRÖK,
*University of Public Administration and Finance Ludwigsburg, Germany*
mueller-toeroek@hs-ludwigsburg.de

Alexander PROSSER,
*University of Economics and Business Vienna, Austria*
alexander.prosser@wu.ac.at

Sven SROKA,
*University of Public Administration and Finance Ludwigsburg, Germany*
sroka_sven@studnet.hs-ludwigsburg.de

## Abstract
In 2021/2022 a consortium of European universities delivered a scientific basis for a policy fighting fake news and hate speech with support of the Congress of Local and Regional Authorities of the Council of Europe, describing also the technical and legal basics of both phenomena. In this context a survey was performed with the delegates of the Congress and the book, which contained also the survey results, was presented to the Congress in its Spring Session 2022. In 2023 a broader survey was done in a selection of countries, which also returned 675 filled-in questionnaires from Romania. The part of the questionnaire dealing with possible remedies contained questions which remedies are considered technically and legally feasible by the participants. Confirming the results of the survey in 2021/2022 the results for Romania showed a severe lack of basic knowledge about how the internet works and its governance. In this paper we want to show the results for Romania in detail, discuss them and suggest possible training measures which seem necessary to make the local and regional politics and administration fit for the Digitalization.The analysis of data from other European countries showed that this phenomenon is not restricted to Romania but is widely recognizable all over Europe. It also confirms the results from the survey among the Congress delegates. Therefore, this paper may be based on the Romanian dataset, *however it signifies a pan-European issue.*The authors are grateful to Vice Dean Nicolae Urs (Babeș-Bolyai University Cluj-Napoca) and Catalin Vrabie (National University of Political Studies and Public Administration) for their support in spreading the survey among Romanian municipalities.

**Keywords:** Digitalization, Fake News, Hate Speech, Human Resources, ICDL.

## 1. Introduction
In autumn 2021 a group of European universities started an initiative with the Congress of Local and Regional Authorities of the Council of Europe (referred to as “Congress” in the subsequent text) to provide European decision-makers, namely national delegations to the Congress and to the Council of Europe with basic information how hate speech and fake news work and how to possibly tackle them. The launching event took place on 8 October 2021 in Strasbourg, [1] the project was presented to the autumn session of the Congress on 27 October 2021, [2] and in the spring session of the Congress the results were presented. [3] The main deliverable was a book titled “Counterfake – A scientific basis for a policy fighting fake news and hate speech” [4], which was also published Open Access.

During the work a questionnaire was distributed online among the delegates of the Congress including youth delegates and delegates from partner countries. It included,

among others, questions regarding technological and legal remedies [5]. “The results indicate that many legislators/policymakers are not aware of the technological feasibilities and restrictions under which the Internet operates.” [6]

However, the original Council of Europe dataset yielded only 187 questionnaires. This of course warranted collection of a larger dataset. To that effect, a group of universities and research institutions repeated the questionnaire in 2023 on a broader base in Austria, Germany, Hungary, Italy, Moldova, Romania, and Slovakia. In this effort, the Romanian dataset was the first one to be available and was hence the “pilot” dataset for the analysis. It contains 675 filled-in questionnaires [7]

In this paper we first present the survey framework and then give an overview of how representatives are affected by hate speech and fake news (Sections 2 and 3). The focus is on the perceived remedies to the issue in Section 4, which analyzes the results regarding technological and legal remedies against fake news and hate speech and draw some conclusions for the necessity of increased digital education of current politicians and civil servants on the local and regional level. For these purposes we describe the questionnaire distributed and its relevant questions in the Romanian version (Section 2), analyze the results and interpret them (section 3) and derive the – likely necessary – vocational training requirements for the Romanian local and regional politicians and civil servants.

**2. The questionnaire used**

The questionnaire is, at least in the relevant questions, identical with the one used in 2021/2022 for the delegates of the Congress. The translation of the question(s) from the English and French master questionnaires was done by Vice Dean Dr. Nicolae Urs (Babeș-Bolyai University Cluj-Napoca) and Prof. Dr. Catalin Vrabie (National University of Political Studies and Public Administration), who were part of the European universities involved.

The online questionnaire was open from February 6, 2023 to May 31, 2023 (for this purpose we stopped on this date, the questionnaire itself remained open till the end of October 2023). The returned 675 questionnaires were from (not all questions answered by respondents):

- 418 females (63.6 %), 238 males and 1 other (cf. [2], p.18)
- 26 local and regional politicians (4 %), 23 mayors (3.5 %) and 608 civil servants (92.5 %) in the administration (cf. [2], p. 18)
- 39 were below 30 years of age (5.9 %), 415 between 30 and 50 (62.3 %) and 212 (31.8 %) older than 50 years (cf. [2], p. 21)
- Overwhelmingly smaller municipalities, 322 of the valid questionnaires from less than 50,000 inhabitants (51.4 %), 210 from entities between 50,000 and 500,000 inhabitants (33.5 %); 95 (15.2 %) came from larger municipalities or regions (cf. [2], pp. 19).

Note that not to answer a question was always an option.

## 3. The Threats

First and foremost, we wanted to gain insight into shape and magnitude of the threat representatives of local and regional authorities are exposed to. The following tables show the results for ten threats we proposed to the respondents. They can be decomposed into "cyber" threats in the digital media (tables 1 to 5) and real, physical threats (tables 6 to 10).

Table 1 Personal insults in media[1]

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 339 | 50.2 | 53.6 |
| | At times | 234 | 34.7 | 37.0 |
| | Frequently | 60 | 8.9 | 9.5 |
| | Total | 633 | 93.8 | 100.0 |
| Missing | System | 42 | 6.2 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

Table 2 Libel in media

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 306 | 45.3 | 49.2 |
| | At times | 247 | 36.6 | 39.7 |
| | Frequently | 69 | 10.2 | 11.1 |
| | Total | 622 | 92.1 | 100.0 |
| Missing | System | 53 | 7.9 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

Table 3 Material damage in media (e.g., cyberattacks against homepage)

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 469 | 69.5 | 78.4 |
| | At times | 118 | 17.5 | 19.7 |
| | Frequently | 11 | 1.6 | 1.8 |
| | Total | 598 | 88.6 | 100.0 |
| Missing | System | 77 | 11.4 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

Table 4 Threats of physical violence in media against the person addressed

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 499 | 73.9 | 83.6 |
| | At times | 89 | 13.2 | 14.9 |
| | Frequently | 9 | 1.3 | 1.5 |
| | Total | 597 | 88.4 | 100.0 |
| Missing | System | 78 | 11.6 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

[1] Including digital, namely Social Media and not restricted to press, TV and radio.

Table 5 Threats of physical violence in media against the family of that person

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 521 | 77.2 | 87.6 |
| | At times | 66 | 9.8 | 11.1 |
| | Frequently | 8 | 1.2 | 1.3 |
| | Total | 595 | 88.1 | 100.0 |
| Missing | System | 80 | 11.9 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

Table 6 Personal insults in the real world

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 313 | 46.4 | 51.4 |
| | At times | 271 | 40.1 | 44.5 |
| | Frequently | 25 | 3.7 | 4.1 |
| | Total | 609 | 90.2 | 100.0 |
| Missing | System | 66 | 9.8 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

Table 7 Libel in the real world

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 340 | 50.4 | 56.0 |
| | At times | 246 | 36.4 | 40.5 |
| | Frequently | 21 | 3.1 | 3.5 |
| | Total | 607 | 89.9 | 100.0 |
| Missing | System | 68 | 10.1 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

Table 8 Material damage in the real world

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 529 | 78.4 | 88.2 |
| | At times | 64 | 9.5 | 10.7 |
| | Frequently | 7 | 1.0 | 1.2 |
| | Total | 600 | 88.9 | 100.0 |
| Missing | System | 75 | 11.1 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

Table 9 Physical violence in the real world against the person addressed

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 552 | 81.8 | 91.7 |
| | At times | 46 | 6.8 | 7.6 |
| | Frequently | 4 | 0.6 | 0.7 |
| | Total | 602 | 89.2 | 100.0 |
| Missing | System | 73 | 10.8 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

Table 10 Physical violence against the family of the person addressed

| | | Frequency | Percent | Valid percent |
|---|---|---|---|---|
| Valid | Hardly ever | 562 | 83.3 | 93.4 |
| | At times | 37 | 5.5 | 6.1 |
| | Frequently | 3 | 0.4 | 0.5 |
| | Total | 602 | 89.2 | 100.0 |
| Missing | System | 73 | 10.8 | |
| Total | | 675 | 100.0 | |

*Source: Author own work*

These tables show a rather depressing result:

- Around 10 % of the respondents are frequently, one third at times confronted with insults or libel in the digital media (Tables 1 and 2);
- Over 1 % are frequently confronted with threats of physical violence or material damage in the digital media, 10 to 20 % at times (Tables 3 to 5);
- Over 3.5 to 4 % are frequently confronted with insults or libel in the real world, over 40 % at times (Tables 6 and 7);
- The percentage of respondents confronted with physical real-world threats or violence frequently is fortunately very low, but 6 to 10 % answered with "at times" (Tables 7 – 10).

This raises some serious questions as to whether it is personally worthwhile to the respondents to engage in public representation on a local or regional level. It may discourage capable and suitable people from becoming a representative, which in turn damages the quality of the political system.

The question arises, whether there is a connection between threats in cyberspace and physical threats/damages.

This was analysed by pairing up the corresponding threats in cyber and the real world, that is 4.1 and 4.6, 4.2 and 4.7, 4.3 and 4.8, 4.4 and 4.9 and finally 4.5 and 4.10. They were subjected to a Pearson X2 test series. All five correlations were significant on a 99 % confidence level. Hence, we may conclude that cyber threats and real-world attacks would go together and that one may easily lead to the other. This is a serious conclusion and the phaenomena may constitute a serious threat not just to representatives but to the political system as such.

## 4. The Proposed Remedies

The questionnaire also asked about perceived remedies to the issue. Here the responses to the remedies proposed.

Table 11 Questions regarding countermeasures

| Question | Yes | No | n/a |
|---|---|---|---|
| 1. Blocking of a web site in my own country | 65.8 % | 23.7 % | 10.5 % |
| 2. Blocking of a web site in another country | 56.4 % | 30.8 % | 12.7 % |
| 3. Identifying and blocking IP addresses of offensive posts in my own country | 80.0 % | 11.7 % | 8.3 % |

| | | | |
|---|---|---|---|
| 4. Identifying and blocking IP addresses of offensive posts in another country | 71.7 % | 17.8 % | 10.5 % |
| 5. Identifying posters of offensive content in my own country | 92.3 % | 7.1 % | 0.6 % |
| 6. Identifying posters of offensive content in another country | 77.0 % | 13.0 % | 9.9 % |
| 7. Blocking email addresses | 67.4 % | 21.8 % | 10.8 % |
| 8. Upload filters to social media platforms | 81.5 % | 9.3 % | 9.2 % |
| 9. Obligation to use clear name in social media | 74.2 % | 16.9 % | 8.9 % |

*Source:* [8]

Regarding the first measure, blocking websites in your own country is technically feasible in general, but with the restriction that the operator of the respective website can find work-arounds, eg. by operating from foreign soil, which leads to the next measure. We should note that in the European Union it is legally feasible but can be used only when fulfilling severe requirements [9].Of course, the term "in another country" includes Member and Non-Member States of the EU; here it is doubtful whether the participants in the questionnaire were aware that common legislation and jurisdiction exists on these topics within the European Union.

Blocking websites in another country is only feasible when an internet regime equivalent to the Great Chinese Firewall is operated [10]. Accessing a website via a VPN or simply a proxy server including the TOR network camouflaging the internet activity, can easily be done by literally everybody [11].

Measures 3 and 4 are both useless, because IP-addresses are typically assigned dynamically by the internet provider. It is also easily possible to hide your IP-address behind another (proxy) server. Many commercial and free offers exist on the internet, one of the most prominent being [12], not to mention the TOR project or more sophisticated tools.

Regarding the fifth and sixth measures, identifying posters of offensive content in your country requires a legally enforceable obligation to use clear names at least to the platform provider and a legal obligation to disclose them, which does not exist in the current European Union legislation [13] . The same applies to other countries. Identification of posters requires more than only the IP address, but also a reliable link between a physical person (consider AI or bots) and this very IP address. It seems as if the respondents are not fully aware of this.

Blocking email addresses, as suggested in the seventh measure, is not useful, simply because impersonating a fake email-address by using a fake sender can be easily done by literally everyone [14] ; there are plenty of fake mail services available on the web.

Upload filters, as suggested in Measure 8 are feasible in theory, but have severe issues, both from a legal and from a technical perspective. Hopes are high concerning application of artificial intelligence; however this technology should not be overrated and still has a large number of false positives [14]. We should also note that an "acting AI" causes legal issues, it is currently at least in conflict with Article 22 GDPR, which states "The data subject shall have the right *not to be subject to a decision based solely on automated*

*processing*, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." [15](cf, our emphasis).

An obligation to use clear names in social media (Measure 9) is feasible in theory, but from a legal perspective several issues occur, the most prominent being: How can a single country "force" platform operators in one of the 192 other countries[2] to use and, in case, disclose clear names? [16]. And, finally, an obligation to use clear names in social media requires the following preconditions:

1. Full and unrestricted cooperation of the social media provider – in all 192 other countries of the world, no matter whether the local legislation permits it or not.
2. A wide-spread and reliable means of identification when registering for a social media account. It is doubtful if e.g. eIDAS-eIDs are recognized by social media platforms in the USA, Russia or China.
3. 100 percent coverage: If a social media platform allows accounts without clear names, people will (ab)use this. Note that even in G7 Member States like Germany it is possible to use e-Government services without providing and means of eID or identification data, which is reliably and safely tied to an identifiable person [17, 18].

This paper focuses on digital literacy, hence the findings analyzed here are also focused on the respective questions. But we have to highlight the definition of fake news as stated by the respondents, which is very interesting:

468 respondents or 69.3 % quoted that "Dissemination of information that can neither be verified nor falsified at the time of dissemination." is perceived as fake news [19]. Hence, as an example, a statement saying "Arsenal will win the Champions League 2023/2024"[3] is fake news – according to the two-thirds majority opinion. Unlike the other questions in the section dealing with the definition of fake news there was no distinction whether this dissemination was done with malign intent or bona fide.

Both fake news and hate speech have been experienced by a significant number of the respondents, fake news personally by 46.7 % and within their institution, 53.2 % whilst hate speech has been experienced personally by 36 % and within their institution by 44.1 % [20]. Summarizing, there is a clear need to improve the representatives' understanding of the digital infrastructure to also improve (i) how representatives respond when they are affected personally and (ii) when representatives formulate legal provisions or strategies against fake news and hate speech on a general political level.

[2] The figure refers to the currently 193 UN Member States based on https://ask.un.org/faq/14345 (as per 2 January 2024) and must in the real world be amended by servers based in regions which are not controlled by a regular UN Member State like the Turkish occupied parts of Cyprus, the Russian occupied parts of Moldova and many more.

[3] As per 3 January 2024, Arsenal is still in the current Champions League season and can probably win it or not, so the statement can neither be falsified nor verified as per this date.

If we take the ICDL[4] as a yardstick and possible solution, the basic concepts of, for instance, e-mail are taught in the basic module "Online Essentials" [21] and, of course, in the good practice module "IT Security" [22]. The question arises why local and regional politicians and civil servants lack basic ICT skills. If we take a deeper look into the answers to this question section, we see that:

- The question regarding the blocking of e-mail addresses shows no significant deviations when testing for the age of the participants. Pearson-Chi-Quadrat stands at 0.044 and we cannot establish a connection between age and the answers – hence we may say that "digital natives" do not show a different response pattern than the older generation.
- The same holds for gender. Pearson-Chi-Quadrat stands at 5.794 and the expected (wrong) answers from females are slightly, but insignificantly lower than we would expect – 274 vs. 281.9 expected.
- Same for Measure 9, the mandatory usage of clear names in social media – we could neither establish a relation between age group and answer, Pearson-Chi-Quadrat 0.224 nor for gender – Pearson-Chi-Quadrat 4.423.

Note again that these findings are not Romania-specific but perfectly in line with the questionnaire collected from the delegates of the Congress of Local and Regional Authorities of the Council of Europe and also in line with our later data collected thus far from AT, DE, IT, MD and SK.[5]

## 5. Conclusion

The overall conclusion is that the digital literacy of local and regional politicians and civil servants, at least in Romania, is quite low and needs to be improved significantly. The same applies to a basic understanding of how the internet works, what an IP address is or how e-mail works is insufficient.

Given the huge figure of currently active politicians and civil servants on these levels, this necessitates a form of vocational training specifically designed for representatives on all levels. For this we strongly recommend the internationally established ICDL program, which is also available in Romania. [23]

It would make sense if the Congress and/or its Member States take action and propose or at least endorse the development of a vocational training program for newly appointed representatives as well as civil servants. Also the definition of standards for such a program (essentially the curriculum) by the Congress would be helpful.

Overall it seems unacceptable for the citizenry that their representatives and civil servants on a local and regional level lack digital literacy – and probably those on a national and supranational level as well.

[4] International Certification of Digital Literacy (ICDL), cf. https://icdl.org/ the official website of the ICDL Foundation.
[5] The data will be published by the beginning of 2024.

## References


[1] "https://www.coe.int/en/web/congress/-/-counterfake-a-scientific-basis-for-a-policy-fighting-fake-news-and-hate-speech," [Online]. Available: https://www.coe.int/en/web/congress/-/-counterfake-a-scientific-basis-for-a-policy-fighting-fake-news-and-hate-speech. [Accessed 18 July 2023].

[2] [Online]. Available: https://www.coe.int/de/web/congress/-/fake-news-and-hate-speech-against-elected-representatives-congress-responds-with-a-project-to-devise-effective-responses;https://rm.coe.int/20211027-en-speech-prof-muller-torok-hate-speech-and-fake-news-on-the-/1680a4. [Accessed 18 July 2023].

[3] [Online]. Available: https://www.youtube.com/watch?v=Oa6tLf_uPm8. [Accessed 18 July 2023].

[4] S. Brüggemann, N. Kutlu, R. Müller-Török, A. Prosser, S. Ručinská, T. Szádeczky and C. Vrabie, "A scientific basis for a policy fighting fake news and hate speech," *OCG/Facultas,* p. 184, 2022.

[5] S. Brüggemann, N. Kutlu, N. Müller-Török, A. Prosser, S. Ručinská, T. Szádeczky and C. Vrabie, "A scientific basis for a policy fighting fake news and hate speech," *OCG/Facultas,* p. 182, 2022.

[6] S. Brüggemann, N. Kutlu, R. Müller-Török, A. Prosser, S. Ručinská, T. Szádeczky and C. Vrabie, "A scientific basis for a policy fighting fake news and hate speech," *OCG/Facultas,* p. 184, 2022.

[7] S. Sroka, "Bildungsstand europäischer Kommunal- und Regionalpolitiker in Bezug auf Fake News und Hate Speech," *sowie Digitalisierung - Auswertung einer Umfrage in Rumänien. Bachelor Thesis at the University of Public Administration and Finance Ludwigsburg,* 2023.

[8] S. Sven, "Bildungsstand europäischer Kommunal-und Regionalpolitiker in Bezug auf FakeNews und Hate Speech, sowie Digitalisierung-Auswertung einer Umfrage in Rumänien," *Bachelor ThesisattheUniversity of Public Administration and Finance Ludwigsburg.,* p. 37, 2023.

[9] C. o. t. E. Parliament, "REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications," *Art.3,lit 3(a).*

[10] S. Brüggemann, N. Kutlu, R. Müller-Török, A. Prosser, S. Ručinská, T. Szádeczky and C. Vrabie, "A scientific basis for a policy fighting fake news and hate speech," *OCG/Facultas,* p. 183, 2022.

[11] S. Brüggemann, N. Kutlu, R. Müller-Török, A. Prosser, S. Ručinská, T. Szádeczky and C. Vrabie, "A scientific basis for a policy fighting fake news and hate speech," *OCG/Facultas,* p. 101, 2022.

[12] [Online]. Available: https://www.hidemyass.com/proxy?nogeoip.

[13] D. Bundestag, "Sachstand Überblick über den aktuellen Diskussionsstand und rechtliche Grundlagen zum Thema "Klarnamenpflicht im Internet"," 21 February 2020.

[14] S. Brüggemann, N. Kutlu, R. Müller-Török, A. Prosser, S. Ručinská, T. Szádeczky and C. Vrabie, "A scientific basis for a policy fighting fake news and hate speech," *OCG/Facultas,* p. 183, 2022.

[15] C. o. t. E. Parliament, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da".

[16] D. Bundestag, "Sachstand Überblick über den aktuellen Diskussionsstand und rechtliche Grundlagen zum Thema "Klarnamenpflicht im Internet"," p. 24, 21 February 2020.

[17] Müller-Török, R. and L. Bader, "Identification issues in citizens' participation Why are eIDAS-compliant means of identification not common standard?," *CEEeGov '22: Proceedings of the Central and Eastern European eDem and eGov DaysSeptember,* p. 118–122, 2022.

[18] R. Müller-Török, "Elektronischer Identitätsnachweis (eID) und elektronische Signatur. Das vergessene Fundament des e-Government"," *PUBLICUS – Der Onlinespiegel für das öffentliche Recht, Boorberg Verlag,* 2022.

[19] S. Brüggemann, N. Kutlu, R. Müller-Török, A. Prosser, S. Ručinská, T. Szádeczky and C. Vrabie, "A scientific basis for a policy fighting fake news and hate speech," *OCG/Facultas,* p. 23, 2022.

[20] S. Brüggemann, N. Kutlu, R. Müller-Török, A. Prosser, S. Ručinská, T. Szádeczky and C. Vrabie, "A scientific basis for a policy fighting fake news and hate speech," *OCG/Facultas*, pp. 6,33, 2022.

[21] I. Foundation, *Online Essentials Syllabus 1.0,* p. 6, 2019.

[22] I. Foundation, *IT Security Syllabus 2.0,* p. 7, 2019.

[23] [Online]. Available: https://www.ecdl.ro/en/article/ecdl-romania_10.html. [Accessed 5 January 2024].