

COVID-19, Infodemic and Cyber Security

Gabriela Belova

Faculty of Law and History
South-West University "Neofit
Rilski"

Blagoevgrad, Bulgaria
gabrielabelova@gmail.com

Gergana Georgieva

Faculty of Law and History
South-West University "Neofit
Rilski"

Blagoevgrad, Bulgaria
georgieva@law.swu.bg

Yosif Kochev

Faculty of Law and History
South-West University "Neofit
Rilski"

Blagoevgrad, Bulgaria
kochev_88@law.swu.bg

Aleksandar Yankov

Faculty of Law and History
South-West University "Neofit
Rilski"

Blagoevgrad, Bulgaria
alexander.yankov1990@gmail.com

Vladimir Babanov

Faculty of Law and History
South-West University "Neofit
Rilski"

Blagoevgrad, Bulgaria
v.babanov@law.swu.bg

Abstract — The present article tries to trace the impact of some processes related to the COVID-19 pandemic on some areas of public life and in particular on national security. The analysis focuses on two main points, namely the infodemic and cybersecurity, as during COVID-19 they stood out as problems that will continue over time. The COVID-19 pandemic has been a challenge that requires the international community, governments and political elites to address multiple dimensions that go beyond just the effects on population health and also have an impact on security aspects. The starting point of the analysis is, of course, the social determinants of the right to health, which promote public health as an element of security and at the same time as one of the goals of sustainable development. In fact, it is precisely some of the determinants of the right to health that are subject to the infodemic, false or misleading information deliberately created to harm a person, social group, organization or country. Furthermore, the weaknesses the pandemic has so far highlighted point to an urgent need for a stronger international framework that would counteract the spread of misinformation and increasing complexity of cyberattacks. That calls for an all-rounded strategy that includes increased international cooperation, public awareness, and the application of cutting-edge technical solutions. An appropriate methodology has been used in view of the delicate matter of health, which becomes even more vulnerable when subjected to infodemic or cybercrime. The main conclusion of the authors is that, in addition to improving international legislation with a view to preparing for and preventing future pandemics, more attention should also be paid to the phenomena that accompany them, such as the infodemic and cybercrime. This is of utmost importance, as they could be expected to develop on a much larger scale in possible future pandemics. The international community and

national elites should discuss and take measures to deal with these phenomena.

Keywords — COVID-19, cybersecurity, infodemic, post-pandemic world.

I. INTRODUCTION

Today, humanity has breathed a sigh of relief that the COVID-19 pandemic is already over. Public health has regained its position and the international community has refocused its efforts on achieving Goal 3 of the Sustainable Development Goals, ensuring a healthy lifestyle and promoting well-being for all during the whole life. However, this does not mean that some aspects related to it, such as infodemic and cybersecurity, should not be carefully analyzed, moreover, they will continue to have an impact on the life of modern society. It is important to follow and outline some trends, as well as the necessity that definite measures should be taken by the international community, by the countries and national elites in order to overcome the negative consequences. This is of utmost importance, as they could be expected to become of greater importance in possible future pandemics.

II. MATERIALS AND METHODS

The present article aims critically to analyze the COVID-19 pandemic health issues in terms of fake news and disinformation as well as cybersecurity.

The issue has been explored in recent years but still needs further attention and research. Due to the sensitive nature of the issue, a complex methodology has been

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2025vol5.8479>

© 2025 The Author(s). Published by RTU PRESS.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

used, combining several approaches and including analytical, teleological, historical and comparative methods.

To achieve the goals of the research, the article also uses some statistical data collected from the official websites of European and national institutions, the observation and analysis of which allows the authors to reach scientifically based conclusions regarding the level of infodemic and cybersecurity.

III. RESULTS AND DISCUSSION

A. COVID-19 and social determinants of the right to health

The UN's Sustainable Development Goals were adopted on September 25, 2015, by the 193 countries in the UN General Assembly as a continuation of the Millennium Goals. Just as they call for a focus on the linkages between development policy sectors, the pandemic has revealed complex global interdependencies that reinforce the lines of ethnic, economic, and gender inequality in society.

Goal No. 3, a part of the agenda 'Transforming our world', has been defined as ensuring a healthy lifestyle and promoting well-being for all during their whole life. Its achievement is directly related to the improvement of the so-called social determinants of the right to health and health care which are mostly understood as structural factors and everyday living conditions that significantly determine existing health inequities within and between countries.

One of the most important determinants of the right to health is undoubtedly nutrition and a healthy lifestyle. The right to health includes not only the provision of a sufficient quantity of safe food, but it also raises the question about the 'double standard' regarding the quality and ingredients of food in some EU Member states, particularly V-4 countries and Bulgaria and Romania as well [1]. In recent years, global prices of basic food products have increased sharply, causing serious concern among the governments of some countries, as well as among non-governmental organizations. According to forecasts of the United Nations Population Fund (UNFPA), by the middle of the 21st century, the population of the planet is expected to reach 9 billion people and lead to a shortage of agricultural land, water, energy resources, food, which in turn would expectedly increase the prices of the main food products from the consumer basket [2]. However, these data and facts regarding the livelihood of the population as one of the most important social determinants of the right to health, have become the basis of a number of fake news related to the pandemic of COVID-19.

B. Infodemic

As Reddy and Gupta rightly point out, in the era of the COVID-19 pandemic there is an abundance of information, leading to the so-called infodemic, and such a situation requires an adequate response and providing people with accurate and verified information [3]. This is

the first pandemic to take place in a time of social media boom, which basically means everyone knows about the coronavirus, everyone is talking about it, and everyone feels able to give some advice about it. The fear associated with the pandemic is unprecedented, so the infodemic may cause more harm than good for public awareness [4], [5]. Some authors even use the term 'netizens' in articles devoted to the pandemic to emphasize the importance of social networks in relation to individuals, equating it to citizenship [6].

It is hardly a coincidence that conspiracy theories of the Malthusian type and a significant portion of the pieces of fake news have emerged on the occasion of the COVID-19 pandemic. The world in the 21st century has noticed a revival of extreme views that wars, epidemics, and diseases keep population growth under control and should be evaluated positively. In the new context of COVID-19, some even portray the Bill and Melinda Gates Foundation as part of a global conspiracy. Bulgaria has not been isolated from the spread of fake news either, and unfortunately, the population has been susceptible to such information. According to a survey conducted in November 2020 approximately 40% of Bulgarians agreed that the coronavirus was a biological weapon created to reduce the population of the Earth and this is relatively a high percentage [7]. Certain internet sites distribute controversial statements by the member of the Chamber of Deputies of Italy, Sara Cunial, who proposes that the International Criminal Court indicted Bill Gates. The Italian newspaper La Repubblica quoted Cunial's May 14, 2020 speech. In her comment on the prime minister, Giuseppe Conte she appeals: "The next time philanthropist Bill Gates calls you, refer him straight to the International Criminal Court for crimes against humanity" [8].

It should be also emphasized that since the outbreak of the COVID-19 pandemic, social media has played an essential role in the genesis of anti-China sentiments around the world. A restaurant chain Kwong Wing Catering in a Facebook message dated January 28, 2020, informed that it will not serve Mandarin-speaking customers as part of anti-epidemic measures [9]. A few days earlier, misinformation that Chinese travelers from Wuhan with fever had slipped through the quarantine at Kansai International Airport was spread on various social media channels in Japan [10]. Conspiracy theories, derogatory attitudes towards eating habits, prejudice against Chinese socio-cultural norms, and calls for the isolation of the entire nation posted on social media are in many cases openly discriminatory and racist in nature. Prolonged stigmatization, stress and multiple mental problems are among the severe consequences of the irresponsible behavior of some media and netizens [6]. In this sense, health service providers, together with mass media, should take responsibility for providing the right information and for creating effective communication with citizens in order to limit the 'infodemic'.

The 'infodemic' proves to be a constantly evolving phenomenon that has led to the appearance of various categories of disinformation. Each of them has a unique

approach and purpose. In this regard [11] points out a systemic classification of fake information which distinguishes three main types. The first one is the so called 'misinformation' which is fake information that is spread without malicious intent. The classic 'disinformation' is fake information which spreads with the purpose of damage infliction. The third type of disinformation, called 'malinformation', is actually a true information which is not meant for public access, but has been openly spread by malicious actors who seek to do harm.

The automation of disinformation generation through the usage of AI in the last few years resulted in a flood of incorrect online content without verifiable sources. Common approach of the malicious actors is mixing and presenting the disinformation in such a way that makes it appear factual. The utilization of satire and parody makes fake information appear harmless but could possibly lead to establishing of fake correlation between unrelated circumstances or people. Misleading content, imposing of imaginary context, fabricated statements and manipulated content are merely a few subcategories in the three classes of disinformation.

In the first days of the COVID-19 outbreak in China, a 'media panic' has been characterized by a flood of fake news and misinformation that has metastasized faster than the coronavirus itself. Not by chance, WHO Director-General Tedros Ghebreyesus on February 15, 2020, during the Munich Security Conference stated that the organization is fighting not only the epidemic, but also the infodemic, which instills fear and panic through uncontrolled rumors and sensational news [12]. The discrepancy with real facts and data was mainly due to online content gleaned from unreliable and dubious but easily accessible social media. Immediately after the outbreak of COVID-19, many bloggers, groups or users on YouTube, WhatsApp, Facebook, Instagram and Twitter began to profit from the popularity of the coronavirus by provoking impulsive and unpredictable actions [13]. Unfortunately, the development of social media is destroying some boundaries that prevent the spread of fake news in democratic countries [14], [15]. As sensational and gruesome content gets the most attention on social media, several users are using COVID-19 to gain cheap popularity or purposefully sow confusion and panic. They provoke mental states such as anxiety, phobia, panic, depression, mania, irritability, delusion about the existence of COVID-19 symptoms and other paranoid ideas. Consumers of health services are too confused and worried not only because of the information about COVID-19 itself, but also because of the behavior of the media actors.

C. Cybercrime

Another challenge to the right to health in the context of the COVID-19 pandemic was cybercrime. As the fears of the coronavirus infection rapidly occupy the minds of the global population, cybercriminals are looking to use every opportunity to extract all kinds of benefits from

their victims on the occasion of services and products related to COVID-19. Cybercriminals, for example, could seek information about treatments, tests or vaccines related to the coronavirus to sell on the black market, encrypt sensitive data and hold it for ransom, or simply disrupt the interoperability of the institution [16]. Interpol Secretary Jürgen Stock stated that hospitals and medical organizations around the world are constantly working to preserve the well-being of individuals affected by the coronavirus who have become targets for ruthless cybercriminals trying to make a profit at the expense of sick patients [17].

The biggest and most disturbing incident to date happened on March 13, 2020, at the University Hospital in Brno (Czech Republic), which suffered an extremely serious cyber attack in the midst of the coronavirus infection epidemic, which led to the suspension of planned operations [18]. As a result of the cyber attack, the hospital was unable to transfer information from key clinical systems to its database and was forced to shut down its IT systems and transfer emergency patients to another medical facility in the city. It should be borne in mind that the hospital was the second largest national site of strategic importance in the field of healthcare and at the time of the attack it was among the most important testing centers for COVID-19 in the Czech Republic. "The public address system at the hospital began repeating the message that all staff should immediately shut down all computers due to a cyber attack", reported a cyber security expert who was waiting at the hospital for surgery at the same time [19]. The cyber attack did not affect work related to coronavirus testing, but it did cause disruption to the hospital's extremely stressful and busy schedule.

Although the exact origin of the attack was unknown, signs point to the possibility that the hospital's IT infrastructure was encrypted by ransomware. The accident was confirmed by the Czech National Cyber and Information Security Agency (NÚKIB), which had been cooperating throughout with law enforcement and hospital staff to succeed in returning the facility to full operational readiness [16].

After the incident in the Czech Republic, experts warn that the spread of the coronavirus infection provides fertile ground for cybercrimes of all kinds. The cyber attack against the hospital in Brno is causing serious concern among specialists, primarily due to the fact that so far online crime related to COVID-19 has been primarily limited to phishing attacks (targeted emails using catchy headlines and attachments to inject malicious software) and disinformation campaigns. After the case of the hospital in Brno, experts warn that the spread of the coronavirus infection provides fertile ground for cybercrimes of all kinds. According to experts, to date, there has never been a cyber attack on a healthcare or medical facility that has directly resulted in loss of life, but it is only a matter of time before it happens [16].

The consequences of the pandemic can only be compared to those caused by the two world wars in the twentieth century. It is assumed that for a better assessment of the situation, it should be analyzed from different points of view. First of all, the health consequences should undoubtedly be taken into account, while in second place are the economic losses. In addition, the sheer scale of the crisis and the impact it is having is naturally causing a lot of fear, uncertainty and anxiety around the world. As some researchers point out, crises usually evoke apathy, conformity, or overenthusiasm associated with some savior [20], [21]. In the case of COVID-19, there are serious psycho-social consequences caused not only by the disease itself, but also by social isolation, disrupted work and family habits, and economic instability. In a survey made in 2020 by the Kaiser Family Foundation, 45% of adults in the United States believe that anxiety and stress related to the coronavirus have had a negative impact on their mental health [22].

D. Post-pandemic situation

Hopes that perhaps with the end of the COVID-19 pandemic and the return to normal life and the normal functioning of state bodies and institutions, cybercrimes in health systems will decrease, unfortunately, did not come true. With technological advances and the deteriorating geopolitical situation, nowadays we are witnessing even an increase in cybercrime. This is a fact even in well-developed democratic countries. As the National Advisor for Cyber security and Risk of American Hospital Association John Riggi stated in 2024 386 health care cyber-attacks were reported [23]. Compared to the previous several years this was the worst year ever for breaches in health care [24]. A careful analysis shows that nowadays ransomware attacks are not just data theft or financial crimes, they become real threat-to-life crimes. A significant part of them threaten the safety of patients in the hospital as they are designed to stop the life support systems, causing maximum delay of medical services or disruption to patient care. Hospitals strongly depend on a third party to deliver critical, life-saving functions and clinical care. In 2023 in the United States due to an attack on third party for health care, a 287% increase in cyber attacks has been reported compared to 2022 [25]. And it should be noted that third-party data breaches pounded health care more than any other sector [26]. And this becomes not an isolated situation in one country but a global concern as the World Health Organization has alarmed that the increased ransomware attacks are putting the world's healthcare infrastructure at critical risk, endangering patient safety and destabilizing healthcare systems [27], [28].

The WHO Director-General Tedros emphasised the severe impact of cyberattacks on hospitals and healthcare services, calling for urgent and collective global action to address this growing crisis. "Ransomware and other cyberattacks on hospitals and other health facilities are not just issues of security and confidentiality, they can be issues of life and death," he said. And added that just as

viruses do not respect borders, nor do cyberattacks and therefore international cooperation is essential [28].

IV. CONCLUSIONS

The COVID-19 pandemic has prompted the international community to take measures and prepare a draft convention on pandemic prevention, preparedness and response in case of possible future pandemics [29], [30]. This is undoubtedly a step forward in the development of international legislation. However, it seems that it is necessary to take timely measures to effectively counter the infodemic and cybersecurity threats, which are likely to increase in future pandemics. While improving international legislation with a view to preparing for and preventing future pandemics, more attention should also be paid to the phenomena that accompany it, such as misinformation and cybercrime. It is the responsibility of all actors – the international community, states and national elites to discuss and to take appropriate measures to deal with these contemporary phenomena.

REFERENCES

- [1] BTA "Bulgarian MEPs Urge European Commission to Take Measures against Double Standards for Foods," Sep. 4, 2017. [Online]. Available: [BTA :: Bulgarian MEPs Urge European Commission to Take Measures against Double Standards for Foods](#). [Accessed Dec. 30, 2024].
- [2] UN Department of Economic and Social Affairs, "World Population projected to reach 9.8 Billion by 2050, and 11.2 billion in 2100". UN Population Division/DESA/UNFRA. [Online]. Available: [World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100 | United Nations](#). [Accessed Dec. 10, 2024].
- [3] B.V. Reddy and A. Gupta, "Importance of effective communication during COVID-19 infodemic." *Journal of Family medicine and primary care*, vol. 9, no.8 pp. 3793-3796, 25 Aug. 2020. [Online]. Available: [Importance of effective communication during COVID-19 infodemic - PMC](#) [Accessed Nov. 15, 2024], <https://doi.org/10.4103/jfmpe.jfmpe.719.20>.
- [4] R. Nikolova and A. Yankov, "COVID-19, Psychosocial Effects and Fake News", International conference Knowledge – Based Organization, Vol.27, Issue 2, pp. 176-179, June 2021. [Online]. Available: ResearchGate, [\(PDF\) COVID-19, Psychosocial Effects and Fake News](#) [Accessed Dec. 16, 2024], <https://doi.org/10.2478/kbo-2021-0069>.
- [5] A. Yankov, "Distinction between the concepts of "freedom of expression" and "hate speech" (In Bulgarian), *International Politics*, vol. 2/2021, pp. 57-64. [Online]. Available: [Publications \(swu.bg\)](#). [Accessed Nov. 15, 2024].
- [6] S. Dubey, P. Biswas, R. Ghosh, S. Chatterjee, M. J. Dubey, S. Chatterjee, D. Lahiri and C.J. Lavie, "Psychosocial impact of COVID-19", *Diabetes & metabolic syndrome*, vol. 14, no 5, pp. 779-788, May 2020. Available: PubMed, [Psychosocial impact of COVID-19 - PubMed](#). [Accessed Nov. 26, 2024], doi: 10.1016/j.dsx.2020.05.035. PMID: PMC7255207.
- [7] BNR "Trend: 40% of Bulgarians believe COVID-19 is a Biological Weapon", Nov. 24, 2020. [Online]. Available: [Trend: 40% of Bulgarians believe Covid-19 is biological weapon - News](#). [Accessed Sept. 17, 2023].
- [8] V. Antonova "Bill Gates, the Villain", [Online]. Available: [Bill Gates, the Villain | AEJ-Bulgaria](#). Jan. 20, 2021. [Accessed Sept. 24, 2023].
- [9] R.Y. Chung and M.M. Li, "Anti-Chinese sentiment during the 2019-nCoV outbreak", *Lancet*, vol. 395, Issue 10225 pp. 686–687, Feb. 12, 2020. [Online]. Available: PubMed, [Anti-Chinese](#)

- [sentiment during the 2019-nCoV outbreak - PMC](#). [Accessed Sep. 17, 2023]. [https://doi.org/10.1016/S0140-6736\(20\)30358-5](https://doi.org/10.1016/S0140-6736(20)30358-5).
- [10] K. Shimizu, “2019-nCoV, fake news, and racism”, *Lancet*, vol. 395, Issue 10225, pp. 685–686. Feb.29, 2020. [Online]. Available: [PubMed, 2019-nCoV, fake news, and racism - The Lancet](#). [Accessed Sep.18, 2023]. [https://doi.org/10.1016/S0140-6736\(20\)30357-3](https://doi.org/10.1016/S0140-6736(20)30357-3).
- [11] J. Harsin, “Disinformation as a Context-Bound Phenomenon: Toward a Contextual Framework”, *Communication Theory* vol. 33, no. 1, pp. 1–23, 2023. [Online]. Available: <https://academic.oup.com/ct/article/33/1/1/6759692>. [Accessed Jan. 21, 2025].
- [12] J. Zarocostas, “How to fight an infodemic”, *Lancet*, vol. 395, Issue 10225, p. 676, Feb.29, 2020. [Online]. Available: [How to fight an infodemic - The Lancet](#). [Accessed Sep.18, 2023]. [https://doi.org/10.1016/S0140-6736\(20\)30461-X](https://doi.org/10.1016/S0140-6736(20)30461-X).
- [13] R.M. Merchant and N. Lurie, “Social media and emergency preparedness in response to novel coronavirus”, *JAMA*. May 26, 2020. [Online]. Available: [PubMed Social Media and Emergency Preparedness in Response to Novel Coronavirus PubMed](#) [Accessed Sep. 26, 2023]. <https://doi.org/10.1001/jama.2020.4469>.
- [14] G. Belova and G. Georgieva, “Fake News as a Threat to National Security”, *International conference Knowledge – Based Organization*, vol. 24, Issue 1, pp. 19-22, June 2018. [Online]. Available: [ResearchGate \(PDF\) Fake News as a Threat to National Security](#) [Accessed Aug. 4, 2022]. <https://DOI:10.1515/kbo-2018-0002>.
- [15] N. Popov, “Globalization and Security of the Individual in the National State”, (In Bulgarian), *Law, Politics, Administration*, vol. 8, issue 2, pp. 10-14, 2021. [Online]. Available: [CEEOL - Article Detail](#). [Accessed Aug. 20, 2022].
- [16] G. Belova, N. Marin and Y. Kochev, “COVID-19 and cybercrimes against healthcare” (In Bulgarian), *National Security*, Issue 5, pp. 34-40, 2020. ISSN 2682-9983. [Online]. Available: https://nacionalna-sigurnost.bg/sdm_downloads/cyber-crimes/. [Accessed Sep.18, 2022].
- [17] INTERPOL “Cybercriminals targeting critical healthcare institutions with ransomware”, Apr. 4, 2020. [Online]. Available: <https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware>. [Accessed Sep.18, 2022].
- [18] Security “Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak”, Mar. 17, 2020. [Online]. Available: [Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak | 2020-03-17 | Security Magazine](#). [Accessed Oct. 4, 2022].
- [19] M. Burges, “Hackers are targeting hospitals crippled by coronavirus”, *Security*, Mar. 22, 2020. [Online]. Available: [Hackers are targeting hospitals crippled by coronavirus | WIRED](#). [Accessed Oct.6, 2022].
- [20] A. Hristova and G. Georgieva, “New Research and Technology Development”, *Kutafin Law Review*, vol.4, Issue 2, pp. 388-397, 2017. [Online]. Available: [New Research and Technology Development: Some Legal and Ethical Issues | Hristova | Kutafin Law Review](#). [Accessed Sep. 18, 2022]. <https://doi.org/10.17803/2313-5395.2017.2.8.388-397>.
- [21] T. Koburov, *Situational foreign political analysis in the field of security*. (In Bulgarian). Sofia, King, 2009, p.109.
- [22] “KFF Health Tracking Poll – Early April 2020: The Impact of Coronavirus on life in America”, Apr. 2, 2020. [Online]. Available: [KFF Health Tracking Poll - Early April 2020: The Impact Of Coronavirus On Life In America | KFF](#). [Accessed Oct. 18, 2022].
- [23] J. Riggi, “A Look at 2024’s Health Care Cybersecurity Challenges”, Oct. 7, 2024. [Online]. Available: [A Look at 2024’s Health Care Cybersecurity Challenges | AHA News](#). [Accessed Nov. 26, 2024].
- [24] J. Riggi, “Ransomware attacks on Hospitals Have Changed”, [Online]. Available: [Ransomware Attacks on Hospitals Have Changed | Cybersecurity | Center | AHA](#). [Accessed Nov. 25, 2024].
- [25] T. Broderick, “Healthcare data breaches hit new highs in 2023”, *Modern Healthcare*, Jan. 25, 2024. [Online]. Available: [Healthcare data breaches hit new highs in 2023 | Modern Healthcare](#). [Accessed Nov. 25, 2024].
- [26] S. Alder, “Healthcare Experiences More Third-Party Data Breaches Than Any Other Sector,” *HIPAA Journal*, Mar. 4, 2024. [Online]. Available: [Healthcare Experiences More Third-Party Data Breaches Than Any Other Sector](#). [Accessed Nov. 26, 2024].
- [27] A. Koceva and D. Kostadinova, “A comparative analysis on apology speech acts in American English and Macedonian”, *PALMK*, vol. 6, no. 12, pp. 37-45, Dec. 2021. [Online]. Available: <https://js.ugd.edu.mk/index.php/PAL/article/view/4757>. [Accessed Jan. 27, 2025]. <https://doi.org/10.46763/palim>.
- [28] V. Mishra, “Cyberattacks on Healthcare: A Global Threat That Can’t Be Ignored”, *UN News Global Perspectives Human Stories*, Nov. 8, 2024. [Online]. Available: [Cyberattacks on healthcare: A global threat that can’t be ignored | UN News](#). [Accessed Dec. 23, 2024].
- [29] Kiryakova-Dineva, Teodora, and Ruska Bozhkova. “Public Health Risk Environment for Bulgarian Smes (Guest Houses and Family Hotels) in the COVID-19 Pandemic.” *Advances in Hospitality, Tourism, and the Services Industry*, pp. 77–102, 2021. [Online]. Available: <https://www.igi-global.com/chapter/public-health-risk-environment-for-bulgarian-smes-guest-houses-and-family-hotels-in-the-covid-19-pandemic/280891>. [Accessed Jan. 30, 2025]. <https://doi.org/10.4018/978-1-7998-6996-2.ch004>.
- [30] Stoykova, P., “Education as a cause for participation in politics: A case study in Bulgaria”. *Balkan Social Science Review*, 18, pp.299–323, 2021. [Online]. Available: <https://js.ugd.edu.mk/index.php/BSSR/article/view/4819>. [Accessed Jan. 31, 2025]. <https://doi.org/10.46763/BSSR2118299s>.